THE BUSINESS CONTINUITY INSTITUTE

GOOD PRACTICE GUIDELINES

(2005)

-

A Framework for

Business Continuity Management

Acknowledgements

The first BCI Good Practice Guidelines (2002) provided the first coherent and comprehensive method for the management of a Business Continuity Programme and was produced by those listed below.

Work Group:
Fred Bell MBCI
Nigel Bridger FBCI
Mark Bryce MBCI
Tim Chadwick MBCI
Chris Green MBCI
Albert Horan MBCI
Phil Slate MBCI
Dr. David J. Smith FBCI
Graham Vingoe FBCI
Pamela White FBCI

Readers:
Lyndon Bird FBCI
Chris Rigby-Smith ABCI
Rolf von Roessing FBCI
David Green FBCI
John Worthington MBCI

Editor:
Dr. David J. Smith FBCI

The new guide has been completely rewritten to take note of:

- The comments received in response to the original guidelines
- The publishing of Publicly Available Specification 56 : 2003 by the British Standards Institution in 2003
- Legislation, regulatory guidelines and practices that have spread Business Continuity implementation into all industrial, public and not-for-profit sectors around the world

Those who have contributed to the new guide include:

Anne Wright MBCI
Ian Griffiths MBCI
Richard Ecclestone SBCI
Martin Lippiett MBCI
James Coates MBCI
Michael Bland MCBI
Jim Barrow MBCI
Julia Graham FBCI
Michael Bews MBCI
Jane Naylor
Howard Booth MBCI
Helen Pettet Affiliate
John Worthington MBCI
Mel Gosling MBCI
Mark Mahoney MBCI
David Bennett MBCI
Elaine Weston MBCI
Colin Ive MBCI
Adrian Jolly Affiliate
Richard Bridgeford MBCI

Coordination group:
Andy Tomkinson MBCI
Jo Welland Affiliate
Ian Charters FBCI
Angela Hobley MBCI
Nathan Bird MBCI
Jeanette O'Neil MBCI

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

Table of Contents

OVERVIEW

Introduction

The BCI published its first Good Practice Guidelines in 2002. The document achieved a wide circulation and was translated into several languages. It also played a significant part in the development of the British Standards Institution's (BSI) Publicly available Specification for Business Continuity Management (PAS 56).

The new Guidelines have been extensively rewritten to take into account the latest thinking in BCM internationally, to recognise a maturity in practice across all sectors, public and private, and to support the current and possible future structure of PAS 56. These Guidelines are dynamic and will change again as they become an input into the PAS 56 revision as it moves towards a British and International Standard under the guidance of the British Standards Institution.

These Guidelines have been developed by members of the Business Continuity Institute (BCI) for the benefit of BCM professionals around the world. We wish to thank them, and their employers, for allowing them the time to contribute to this guide.

Objective

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

There is a close and converging relationship between the GPG and PAS 56 as both develop. It is intended that PAS56 defines the requirements of a BCM programme and that where the Specification calls for a process, these Guidelines provide more detail on how that process may be undertaken.

Audience

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

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

These guidelines are therefore intended for use by BCM practitioners, risk managers, auditors and regulators with some knowledge of BCM principles. They are not intended to be a beginner's guide as that would have to be much more detailed. Newcomers to the discipline should work alongside an experienced practitioner or attend an appropriate selection of the many BCI-endorsed BCM courses.

What is Business Continuity Management (BCM)?

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

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

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

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

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

The Case for Business Continuity Management

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

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

In managing any event, a successful outcome is judged by both the technical response and the perceived competence of the management. Research by Knight and Pretty (see reference list) indicates that organisations affected by catastrophes fall into two distinct groups - recoverers and non-recoverers. Where an organisation has successfully dealt with a crisis their share value has increased in the long-term in contrast to those who were perceived not to have managed the crisis well whose share price declined and, after a year, had still not recovered.

A key feature of successful BCM programmes is that ownership of the various responsibilities has

been taken at the appropriate levels in the organisation. In these organisations BCM implications are considered at all stages of the development process of new projects and the BCM implications are part of the change control process.

How will it benefit my organisation?

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

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

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

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

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

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

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

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

Relationship with other specialist disciplines

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

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

Table : Comparison on Risk Management and Business Continuity Management

	Risk Management	*Business Continuity Management*
Key Method	Risk Analysis	Business Impact Analysis
Key parameters	Impact & Probability	Impact and Time
Type of incident	All types of events - though usually segmented	Events causing significant business disruption
Size of events	All sizes (costs) of events - though usually segmented	For strategy planning : Survival threatening incidents only
Scope	Focus primarily on risks to core-business objectives	Mostly outside the core competencies of the business
Intensity	All from gradual to sudden	Sudden or rapid events (though response may also be appropriate if a creeping incident becomes severe)

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

Relationship of GPG to other guidelines and standards

The relationship between the GPG and PAS56 has been outlined above.

Other standards with BCM elements are:

- BS 7799 – Although primarily an information security standard there are aspects of Business Continuity provision which must be covered in order for BS 7799 to be fully implemented.
- ITIL – This standard concerns itself with the provision of Service Management disciplines for example Risk and Security, Change, Problem, Configuration, Capacity and Availability however there is a link between the ITIL IT Service Continuity (Disaster Recovery) and Business Continuity.
- Rules and Guidelines such as those outlined in Sarbanes-Oxley and Basle II, influence BCM by mandating its implementation and setting service continuity parameters

Using the Guidelines

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

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

Even so it is recognised that there may be a case where the process outlined may need to be modified to meet the specific needs of an organisation. Therefore each organisation needs to

assess how to apply the guidelines to their own organisation. They must ensure that their BCM competence and capability is appropriate to the nature, scale and complexity of their business, and reflects their individual culture and operating environment.

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

Scope of the Guidelines

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

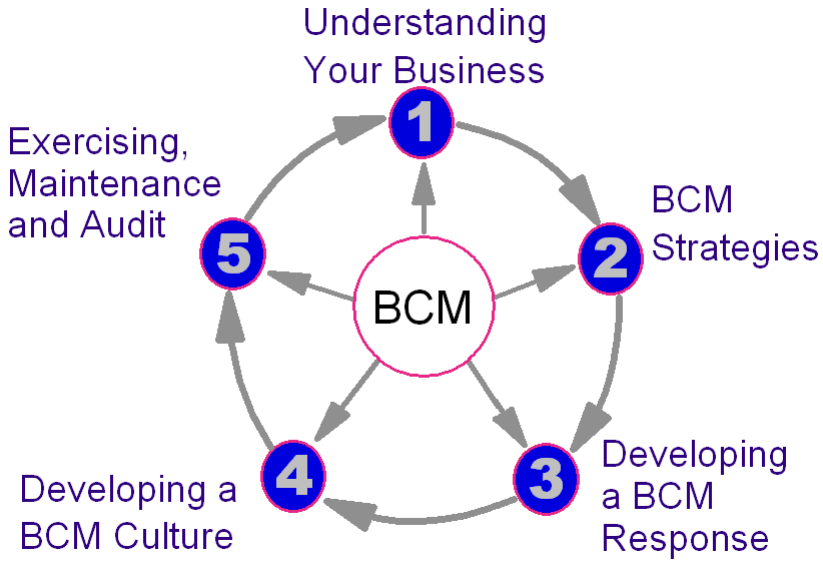
The Guidelines therefore focus on the primary role of the BCM practitioner and assume that specialist in other disciplines (IT, security, HR and the business) will be available to advise on the implementation of these aspects.

Layout of the Guidelines

The Guidelines follow the Business Continuity Management Life Cycle ; starting with Programme Management, then following the Cycle from Stage 1 to Stage 5.

Though this model demonstrates how the stages fit together intellectually, in practice the experienced practitioner will not necessarily follow this progression strictly. For example a 'scenario-based' exercise (Stage 5) may provide 'buy-in' at the start of a programme and plans may be written to provide incident-readiness for the most 'critical' functions before requirements for other functions in the organisation have been investigated. However progress should always be measured against the whole life cycle and across the whole organisation.

Figure: The Business Continuity Management Life Cycle



The Business Continuity Management Programme:

- Organisation (Corporate) BCM Strategy and BCM Policy.
- Business Continuity Management
- Incident Readiness and Response

Stage No.1: Understanding Your Business:

- Organisational Strategy
- Business Impact Analysis.
- Risk Assessment and Control.

Stage No.2: Business Continuity Management Strategies:

- Organisation (Corporate) BCM Strategy.
- Process Level BCM Strategy.
- Resource Recovery BCM Strategy.

Stage No.3: Developing and Implementing a BCM Response

- Crisis Management, Public Relations and the Media.
- Business Continuity Plans
- Business Unit Plans, Incident Response

Stage No.4: Developing a Business Continuity Management Culture

- Assessing
- Designing and delivering
- Measuring results

Stage No.5: Exercising, Maintenance and Audit

- Exercising of BCM plans.
- BCM Maintenance.
- BCM Audit.

Structure and Format of the Guidelines

Each stage contains of:

Guideline Stage	Questions answered
• Introduction	
•Skills required	What BCM skills are required for this stage
•Three components	Contents described below

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

Guideline Component	Questions answered
•Introduction	
•Precursors	What needs to be done before this?
•Purpose	Why do we need to do it? What will it achieve?
•Concepts and Assumptions	What do we need to understand? What assumptions are we making?
•Process	What do we need to do?
•Methods and Techniques	What are the tools we need to do it?
•Outcomes and Deliverables	What should it produce?
•Review	When should it be done? (This may be moved to PAS56)
•Evaluation Criteria	How do we know if we have got it right? (These are now in PAS56)

Source References and Further Reading

As indicated earlier the guidelines incorporate the collective experience, knowledge and expertise of many leading professional Members and Fellows of the Business Continuity Institute (BCI) that are currently engaged within the many sectors.

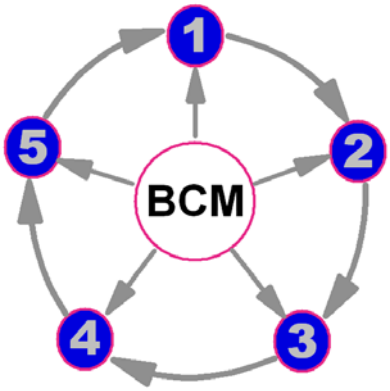
Details of further reading both general and related to a specific section are provided in an Appendix. Where possible details of case studies and videos are also identified.

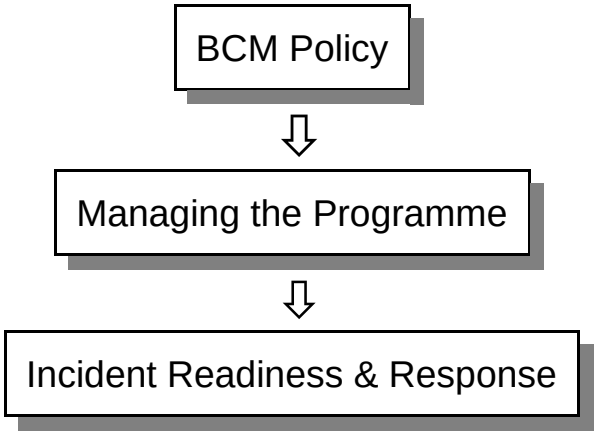
Feedback

All constructive feedback in respect of the guidelines is encouraged and welcomed as it provides a valuable source of comment that will improve the guidelines.

Any feedback or suggestions concerning additions or alterations to the content, style and/or structure of the workbook should be sent to the Business Continuity Institute (lorraine.darke@thebci.org) for consideration and possible inclusion.

Business Continuity Management





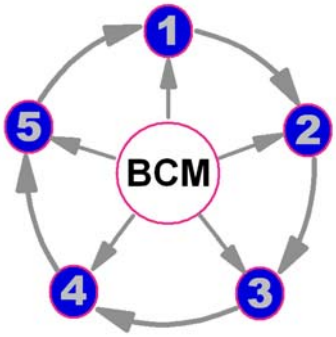
Introduction

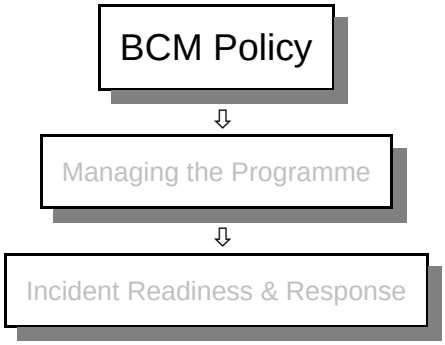
To be effective Business Continuity Management (BCM) must be an accepted management process driven from the top of the organisation. It has to be set out in a vision statement that is fully endorsed and actively promoted by the Executive – this is formally known as the BCM Policy for the organisation.

A member of the Executive should be given overall accountability for the effectiveness of the organisation's BCM capability. This ensures that a BCM programme is given the correct level of importance within the organisation and a greater chance of effective implementation. Regulatory Authorities such as the UK Financial Services Authority (FSA) consider that BCM is a cost of doing business and needs to be funded properly.

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

BCM Policy





Introduction

The BCM Policy of an organisation provides the framework around which the BCM capability is

designed and built. It is a documented statement by the organisation's executive of the level of importance that it places on BCM.

Purpose

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

Concepts and Assumptions

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

Process

The process to develop a BCM Policy include:

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

Methods and Techniques

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

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

issues and drivers.

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

Outcomes and Deliverables

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

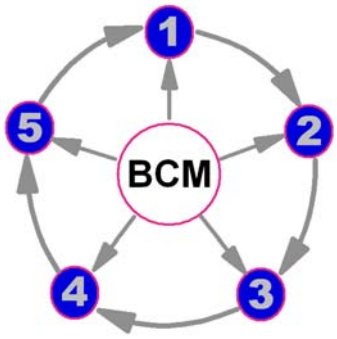
- The organisation's definition of BCM
- A documented set of BCM Principles, guidelines and minimum standards
- A documented BCM Operational Framework for the management of the organisation's BCM programme

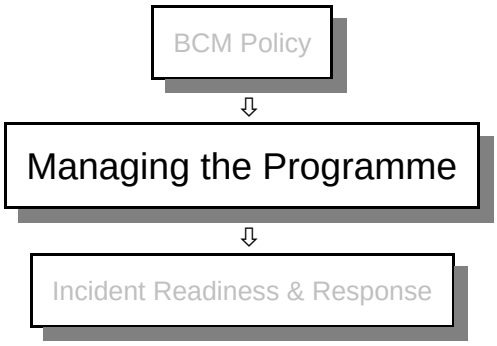
An implementation plan for the Policy.

Review

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

Managing the Programme





Introduction

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

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

Purpose

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

Concepts and Assumptions

Staffing

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

In smaller organisations the BCM function may be given to an individual along with other roles. This is rarely satisfactory where another role involves daily operational responsibility.

Process

The Executive of the organisation should:

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

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

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

Methods and Techniques

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

- These Good Practice Guidelines
- A BCM Policy self assessment scorecard
- Annual Personal Performance Contracts and Appraisals
- Supplier and outsource provider relationship management of business services and products
- Supplier relationship management of BCM specialist resources and services
- Financial management.

- Legal and regulatory advice.
- Industry BCM Benchmarking (Process and Metrics)
- National and International Standards such as the BSI's PAS56
- Internal and/or independent BCM audits
- Cost benefit analysis.
- Review and challenge.

Outcomes and Deliverables

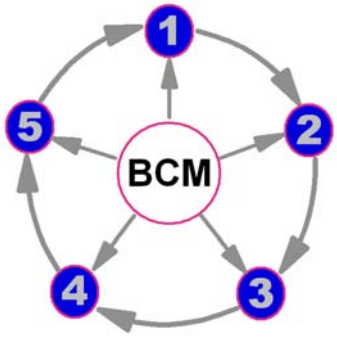
The deliverables of the BCM programme include:

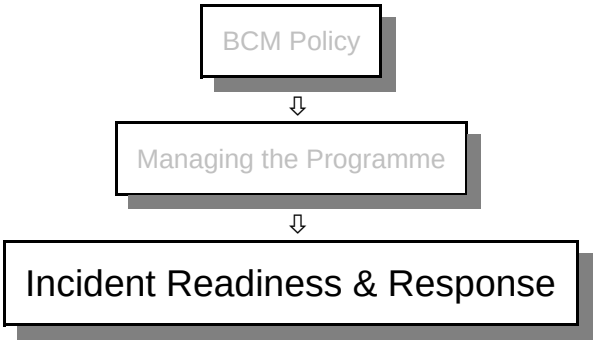
- A clearly defined and documented BC management programme that is agreed by the organisation's executive/senior management.
- BCM assurance reports at a predetermined frequency
- Clearly defined and documented BCM Strategy and Standards
- A management process that is an integral part of the organisation's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

Review

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

Incident Readiness and Response





Introduction

Though Business Continuity Management is primarily a planning activity, it is inevitable that the BC team will be expected to provide a lead during incident response.

Purpose

To maintain a state of readiness so that incident management takes over smoothly to put into action the required plans.

Concepts and Assumptions

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

Process

- Receive notification of problem
- Assess situation then
  - Either manage response through appropriate prepared plans
  - Or escalate to crisis management team
- If a response is required then immediate things to consider include:
  - Are you physically and emotionally fit to assist or lead a response
  - Are the others from whom a response is required present and able to undertake the roles assigned to them - some people may react to an incident with unusual behaviour
  - Have you communicated what has happened to senior management

Methods & Techniques

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

- Contain - Is there anything that can be done immediately to stop the problem getting worse
- Look at the Plan - Is there a pre-planned response that fits this incident?
- Follow the documented procedure which may include the following steps:
  - Communicate - Trying to solve the problem on your own may waste time if the situation then gets out of control.
  - If necessary assemble a team to respond to the incident
  - Assess the situation - Find out as much as you can without putting yourselves at risk
- Predict the likely outcome - and adapt the BC Plan to provide a response strategy

- Predict a 'worst case' outcome - and have a 'back-up' response strategy
- Escalate the response to the required level within the organisation
- Implement the response strategy
- Evaluate the progress of the response against the likely outcome
- As soon as the situation allows, review the effectiveness of the response

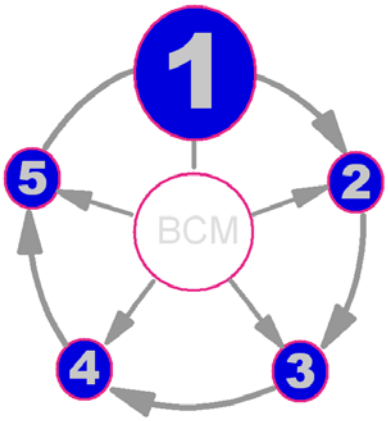
Outcomes and Deliverables

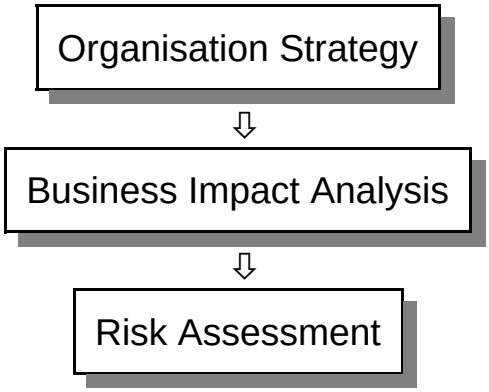
The outcome of a successful response is a controlled return of the organisation to business as usual.

Review

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

Stage 1: Understanding Your Business





Introduction

To be able to develop an appropriate Business Continuity Management programme you must first understand your business and what activities or processes are essential to ensure continuity of business critical activity to at least a minimum level.

These questions need to be asked:

- What are the objectives of the organisation?
- How are the business objectives achieved?
- What are the products/services of the organisation?
- Who is involved (both internally and externally) in the achievement of the business objectives?
- What are the time imperatives on the delivery of the products or services?

The first questions are standard to business analysis, but the last one is central to the analysis for Business Continuity purposes.

The understanding must be focussed on the activities, which most quickly threaten the achievement of business objectives. These tend to be the 'operational' functions, which interact directly with customers or other outside organisations. However these activities may depend for their delivery on the 'support' of other internal and external process, which must also be analysed.

Organisation function types:

- Examples of operational functions include:
  - Customer service
  - Sales
  - Production
- Examples of support functions include:
  - IT
  - Human Resources.
  - Supply Chain

- Strategic activities include:
  - Management
  - Projects
  - Planning

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

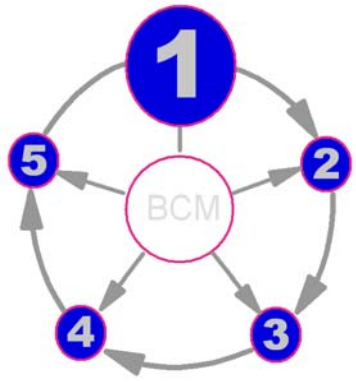
- Business Impact Analysis (BIA) - a mandatory tool forming the foundation for the selection of recovery strategies and plans
- Risk Assessment (RA) focussing on specific functions and known threats

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

The business functions identified as part of the BIA as in need of most urgent resumption are sometimes termed 'Mission Critical Activities' however, unless the organisation is undertaking unnecessary activities, it must be assumed that all major business processes need to be resumed at some point. However, at least to start with, an organisation should focus its BCM effort on those in most urgent need of resumption, termed in this guidance 'critical business functions'.

Risk Assessment (RA) activity helps in identifying potential causes of interruption to an organisation, the probability of occurrence and impact of the threat being realised. Within the BCM programme, a RA should focus on the specific technologies and inherent risks of the business functions identified as most urgent in the BIA results rather than on all risks to the organisation.

1.1 Organisation Strategy



Introduction

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

A Business Impact Analysis is conducted without reference to an interruption cause. However it is necessary to decide on a number of generic scenarios which may result in interruption to business against which the impact of the interruption can be assessed. This should take into account the scope set down in the organisation's own BCM Policy and should where possible take in to consideration planned business change.

Precursors

A documented Business Continuity Management (BCM) Policy.

Purpose

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

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

Concepts and Assumptions

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

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

Process

Steps to identifying the organisational strategy are:

- Review, and challenge if necessary, the scope set out in the BCM Policy
- Decide on the maximum extent of an interruption that the organisation wants to, or needs to, plan to survive. This could be determined by:
    - Geographical extent (or market/customer area)
    - Regulatory or statutory requirements
    - Products, market sectors or specific customers
    - Specific interruption scenarios – such as computer failure or denial of access

This will result in a series of high-level scenarios against which a BIA can be conducted that may include:

- Loss of staff
- Loss of location (single and/or multiple)
- Telecommunications failure
- Computer system failure (component and/or total)
- Equipment failure (e.g. depending on industry: building management systems, manufacturing capacity)
- Supplier failure

The number of scenarios against which BIAs are undertaken is very much the choice of the organisation. Their scope may be modified as activity progresses to either increase or reduce the number of scenarios. It should also be remembered that certain scenarios can encompass multiple scenarios, e.g. loss of a building may include loss of staff, voice & data systems, key documentation, etc.

Methods and Techniques

Key tools to assist:

- Outline understanding of the organisation's 5 year plan
- Current management information outlining process details, volumes, targets and, where possible, quantified value of the activity

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

Outcomes and Deliverables

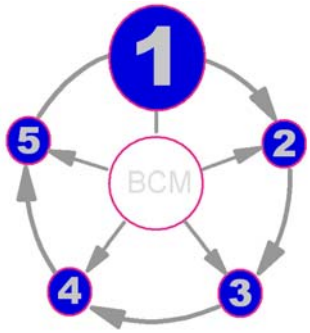
- A scope and terms of reference document for the Business Impact Analysis and Risk Assessment.

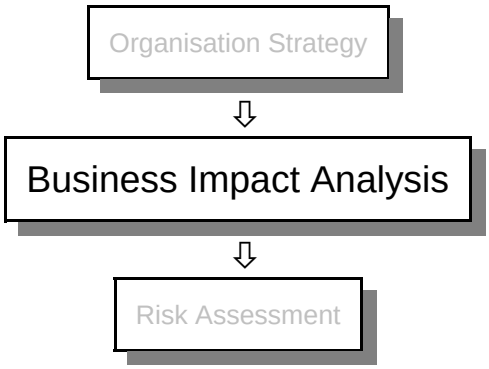
Review

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

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

1.2 Business Impact Analysis (BIA)





Introduction

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

Precursors

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

Appointment of a project sponsor and champion from within the Executive or Senior Management Group is essential.

Purpose

The purpose of a Business Impact Analysis is to:

- Obtain an understanding of the organisations most critical objectives, the priority of each and the timeframes for resumption of these following unscheduled interruption.
- Inform a management decision on Maximum Tolerable Outage for each function
- Provide the resource information from which an appropriate recovery strategy can be determined / recommended
- Outline dependencies that exist both internally and externally to achieve critical objectives

Concepts and Assumptions

Concepts

- Maximum Tolerable Outage (MTO) - this is the timeframe during which a recovery must become effective before an outage compromises the ability of the organisation to achieve its business objectives and therefore has the potential to threaten its short or long term survival
- Seasonality may affect the MTO. As examples, a financial year end may reduce the tolerable

outage for the finance function and a one-off contract with significant time penalties may reduce the tolerable outage for a range of functions within the organisation.

- Recovery Point Objective (RPO) - is the point to which information must be restored to ensure business objectives can be met in line with maximum tolerable outage for the activity

Assumptions

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

Process

Scope and Scale

- If the organisation is part of a group – identify the relationship between the various parts of the organisation
- If the organisation has multiple locations identify the geographical scope of the BIA
- Identify the key business objectives and success criteria of each
- Confirm the incident scenarios to be investigated (see previous section)
- Sign off the terms of reference with the project sponsor drawn from Executive or Senior Management Group

Business Impact Analysis

- Identify discrete business processes across the organisation (which may cut across several departments) and management owners of these processes
- Identify suitable staff from whom information can be sought about the business processes – subject matter experts
- Identify the impacts which may result in damage to the organisation's reputation, assets or financial position
- Quantify the timescale within which the interruption of each business function becomes unacceptable to the organisation

Resource Requirements

- Quantify the resources required over time to maintain the business functions at an acceptable level and within the maximum tolerable outage period

Reporting

- Obtain sign-off by the process owner to confirm accuracy of information

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

Methods and Techniques

Data collection

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

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

As a general guideline:

- Workshops can provide rapid results and an opportunity for hands-on engagement with the programme provided there is consistent buy-in from all departments and participants
- Questionnaires provide large amounts of data but information quality can be very questionable if not completed with consistency
- Interviews can provide very good information but are time consuming and output can vary in format and detail
- Combinations of the above methods can provide excellent results providing an appropriate level of detail and a standard reporting format which will assist in consistency of recording and analysing information across multiple functions.

Data Collection Questionnaires

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

- What is the aim of the BIA?
- How will the information collected be used?
- What is the best format of data collection to report results effectively?
- What basic information is needed to establish criticality of the activity being analysed in isolation and as part of the organisation as a whole:
    - Timeframes within which the activity must be resumed
    - Locations from which activity is undertaken
    - Influences on the activity, e.g. what can impact the activity, peak periods, regulatory reporting
    - What is the impact of not continuing the activity and how long can the organisation last without it (are there any alternatives?)

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

Resource requirements analysis

Resource requirements analysis as part of the BIA process quantifies minimum requirements e.g. people, technology, telephony, etc., following an interruption to support continuity of each business process at a tolerable level of service. The resources required to operate a function at an alternative location may all be required at the same time or be phased in over a period.

Note that some functions (e.g. call centre) may require additional staff (above the normal complement) to deal with backlogs and extra tasks especially if relocation involves additional travel to work time and limited functionality of systems or equipment.

Software

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

Reporting

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

Outcomes and Deliverables

The outcomes from a Business Impact Analysis are:

- A statement of Organisational aims and objectives
- The timeframe within which both financial and non-financial impacts on those aims and objectives as a result of the disruption on each business process (Maximum Tolerable Outage) will be realised
- Resource requirements over time to enable each business function within the organisation achieve continuity or resumption of activity within the timeframes established as part of BIA activity. It will identify:
  - Staff numbers and key skills
  - Vital Records and data currency (Recovery Point Objective)

- Voice and data applications and systems
- Infrastructure (cabling and network links)
- Facilities (alternative location needs)
- Suppliers (intra-organisation and/or outsourced providers) and their interdependencies
- Constraints (such as contractual issues)

This information feeds directly into the Recovery Strategy stage.

- The Organisation Aims will set the scope and scale of the Recovery Strategy.
- The MTO and resource requirements will provide the data to evaluate alternative recovery solutions for adequacy
- The RPO will determine the appropriate information back-up strategy for the organisation

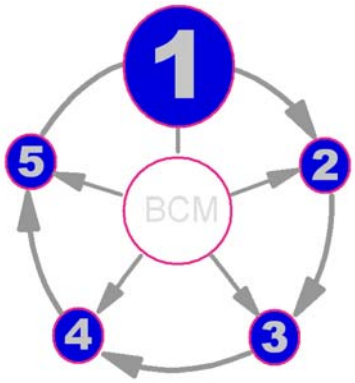
Review

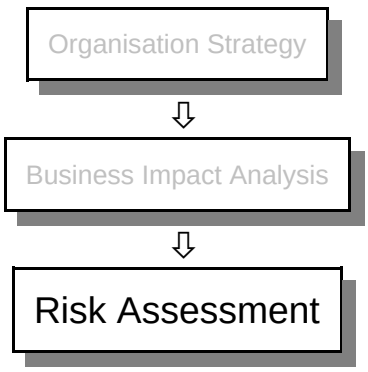
Good practice indicates that a Business Impact Analysis should be reviewed as a minimum annually but more frequently in the event of:

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

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

1.3 Risk Assessment (RA)





Introduction

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

Risk Assessment activity should be focussed on the most urgent business functions identified during the BIA process.

It is recognised that Risk Assessment has serious shortcoming in evaluating catastrophic operational risks because it is impossible to identify all threats and estimates of probability are guesswork or based on historic and sometimes inaccurate information. However, by focussing on the most urgent functions, the scope of the Risk Assessment can be reduced to a more manageable scope.

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

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

Precursors

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

Purpose

The Purpose of a Risk Assessment is to:

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

Concepts & Assumptions

Concepts:

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

- Risk = Threat impact * Probability

Some risk models then order risks by: Priority = Risk * Ability to control that risk. This prioritises the threats that are easiest to control with, presumably, the argument that this will give the best return on investment of time and money but ignoring many external impacts.

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

The organisation's 'risk appetite' or 'risk tolerance' is the amount of risk that an organisation is

prepared to accept and drives the level of action it will take to control identified threats.

Assumptions

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

Process

The key stages in a Risk Assessment are:

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

Methods and Techniques

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

Determining threats

- Event Tree Analysis
- Fault Tree Analysis

Assessing probabilities

- Insurance statistics
- Published disaster frequency statistics
- Local and industry knowledge

Scoring systems

There are examples of scoring systems for impact, probability and ability to control in the Appendix of Sample Documents.

Tabulating Threats

- Threat Vulnerability Matrix - there is an example in the Appendix of Sample Documents
- Risk Quartile Matrix

Evaluating solutions

- Cost Benefit Analysis.

Outcomes & Deliverables

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

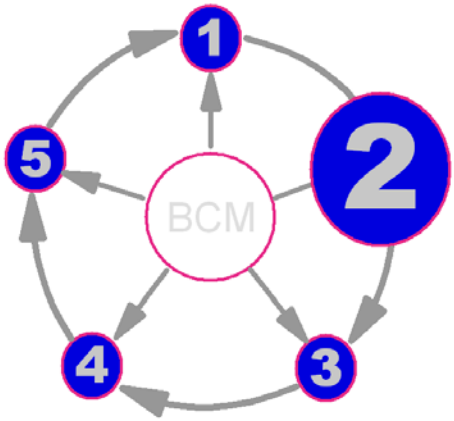
- Single points of failure
- Prioritised list of threats to the organisation or to the specific business processes analysed
- Information for a risk control management strategy and action plan for risks to be addressed
- Documented acceptance of identified risks that are not to be addressed

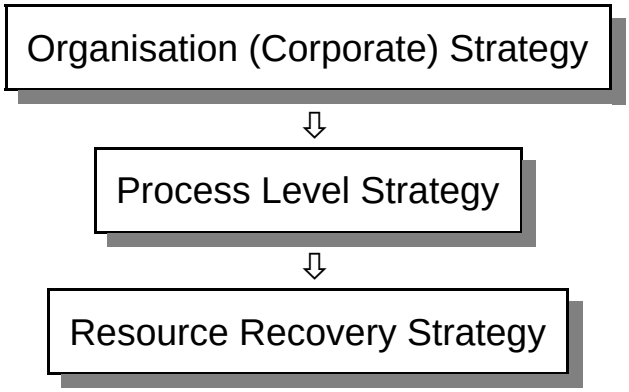
Review

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

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

Stage 2: BCM Strategies





Introduction

This section is about determining and selecting Business Continuity Management Strategies to be used to maintain the organisation's business activities and processes though an interruption.

Business Continuity Management Strategies concern:

- the selection of alternative operating methods to be used after an interruption to maintain the organisation's business critical processes and their dependencies (internal and external) to a priority, and time table determined in the Business Impact Analysis
- the protection of vulnerabilities and single points of failure in business critical processes identified in the Risk Analysis

There are three levels of BCM strategy and strategic planning that need to be considered:

- Organisation (Corporate) Strategy

  An organisation strategy framework providing policy that reflects the key business, stakeholder, legislative and regulatory requirements

- Process Level BCM Strategy

  The resumption strategies for business processes and activities

- Resource Recovery BCM Strategy

  The deployment of appropriate resources to ensure appropriate continuity across all business processes and activities

Strategy Options and Considerations

Introduction

The Business Impact Assessment provides the information from which to choose an appropriate strategy because it identifies the point at which the organisation's survival is threatened by an interruption (Maximum Tolerable Outage - MTO). The organisation may then set a (shorter) Recovery Time Objective that gives a margin of error on the MTO. A strategy that cannot meet the MTO is certain to fail if implemented, but one that exceeds the RTO significantly may be

unnecessarily costly (unless it can be justified for other reasons).

There are a number of generic strategies to mitigate the impact of a disruption or reduce the probability of a threat event. Each strategy has parameters of speed of resumption, reliability of availability and cost which will be appropriate to different parts of the business so an organisation may require several elements to form an appropriate solution, depending upon the individual business functions.

Measures providing functional relocation

- A **'do nothing'** strategy may be acceptable for certain non-urgent functions identified in the BIA. Purchasing buildings and installing utilities may take several months
- **Budge up** makes use of existing in-company accommodation such as a training facility or canteen to provide recovery space or increasing the office density. This will require careful planning and some technical preparation.
- **Displacement** involves the displacing staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent work suspended do not become unmanageable.
- **Remote Working** includes the concept of "working from home" and working from other non-corporate locations e.g. hotels (Internet Cafes should not be considered). Working from home can be a very effective solution but care must be taken to ensure Health and Safety issues are addressed and sufficient dial-up capacity is available.
- **Reciprocal agreements** can work in some selected services but care must be taken when establishing this type of agreement. Procedures must be in place to ensure that periodic checks are performed to ensure that the required arrangements have not changed. Reciprocal agreements must have a clause in the contract to ensure that testing is allowed.
- **Third party alternative site** arrangements from a commercial or service company may be an option for consideration if these can ensure the organisation's recovery time objectives (RTO) are achieved. There are a range of commercial services including fixed, mobile and prefabricated sites.
    - **Dedicated space** provides guaranteed and immediate availability but is more expensive than syndicated space.
    - **Syndicated space** usually provides access within 4 hours but may take more than 48 hours for a large number of staff to become productive from the site *(Issues with syndication are discussed under Concepts)*
    - **Mobile facilities** can be in use rapidly but provide limited space and may require service connections and significant preparation of foundations
    - **Prefabricated** units take a minimum of 4 days to build (average 8) assuming pre-prepared foundations and depending on site and weather conditions
- **'Ship in' Contracts** includes generators, IT equipment such as PCs, servers and printers and specialist hardware and equipment such as telephony systems. This may be an appropriate strategy if an unprepared building is to be equipped to provide an appropriate working environment. Most ship-in contracts permit the delivery location to be nominated at invocation, allowing a more flexible response to a specific incident compared to a fixed site recovery capability. Contract terms vary from 'best efforts' to guaranteed delivery.

- **Resilient Operations** include dual site operations and continuous availability solutions. In the event of an interruption at one site the business function is transferred to one or more alternate locations at which staff and facilities are already prepared to handle it. These options are normally amongst the more expensive to implement but provide the appropriate solution where quick resumption is necessary. To be a viable recovery strategy this configuration should have no single points of failure and an appropriate geographical separation and diversity of the two or more sites.

Figure : Summary of Relocation Strategies against recovery time

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

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

Issues with specific business services:

- **Data Centre(s)** BCM strategy and solutions must be agreed at an Organisation (Corporate) Level. The cost of the solutions and the widespread impact of that the loss can have a major financial impact on an organisation.
    - There are a number of options that can provide a suitable solution including in-house resilience, recovery or third party support.
        - **Technology Duplication** at separated locations is required when resumption timescales are tight, but increases in expense according to the degree of duplication.
        - **Technology Recovery** provides replacement through third-party contracts
            - The decision as to whether to duplicate or contract hardware in advance or acquire

post-incident must take into account the expected lead-time for acquiring the items in a widespread incident which may be long when less-prepared organisations may be chasing the same equipment. Verbal promises by a supplier to keep a contingency stock should be treated as non-contractual.

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

- **Telephony,** the unplanned redirection of telephony to alternative locations may not be possible within an acceptable timescale particularly during wide-area events. Most telecommunications operators will offer, for a charge, a range of flexible planned solutions that will allow instantaneous or rapid redirection of calls from one site to one or more alternatives. The logistical problem of handling telephone calls during an interruption, once they have been redirected, needs to be addressed.
  - Techniques include:
    - Broadcast notification to staff and other stakeholders
    - Call diversion
    - Resumption plan
    - Managed network services
    - Mobile switchboard
    - Site resilience
    - Network resilience
  - The convergence of telephony and data networks VOIP (Voice over IP) creates new opportunities and continuity issues, These issues need to be assessed and the risks and impacts thoroughly analysed.

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

- **Electronic Commerce and Internet / Intranet** strategies will have a choice based on how the whole organisation views the importance of these services and the role they play - whether for communication only or for interactive business.
  - The resumption parameters of Electronic Commerce Services need to be determined by a Business Impact Analysis in the same way as other functions. Electronic Commerce Services are often seen as needing rapid resumption because of their visibility and customer expectations.
  - The Internet and Corporate Intranet may also provide an excellent vehicle for communications during an incident.

- **Manufacturing solutions**
  - **Geographical diversity** – manufacturing at more than one site increases resilience to a

variety of events but is usually at the expense of economies of scale

- **Subcontracting** - Though each company's total process may be unique, there are usually various processes which can be duplicated by other manufacturers. The affected company can then use a number of subcontractors to produce the usual finished product whilst their own facilities are unavailable. This can rarely be achieved quickly without advance preparation due to the need for tooling and set-up. Unfortunately this strategy may introduce your customers to your competitors.
- **Warehousing stock** – For products that can be stored, an off-site stock can provide a time window in which supply can be maintained while a disruption is resolved

- **Supply chain solutions include**:
  - Dual sourcing of materials where interruption of supply would rapidly halt production
  - Holding inventories off-site - at another site or at the supplier's site
  - Significant penalty clauses on supply contracts (though this will not protect against bankruptcy)
  - Inspection of supplier's business continuity plans and test performance record
- **Off-site storage** of paper and electronic records. These are best negotiated at a corporate level ensuring the best value for money through economies of scale. The storage site should be sufficiently far away to ensure that they are not also affected by an incident, but not so far that access takes so long that MTO's are threatened. The RTO of the function using the records will determine the suitable back-up strategy. Some papers may be work-in progress and be required in short timescales whilst other may be archives retained for legal or regulatory purposes for which deep storage, at lower cost, will be suitable.
  - **Paper records off-site storage s**olutions include off-site battle boxes, fire-'proof' cabinets, and optical copies.
  - **Electronic record storage** can be managed in-house but are also provided by a range of suppliers. Records can be sent off-site by physical collection of storage media or by electronic transmission.

Other strategies

- **Outsourcing.** More and more organisations are outsourcing business critical processes and activities to create virtual organisations. It is critical to remember that the risk to the organisation's reputation and brand image cannot be shifted to either intra-organisation sourcing or outsourced providers ; the risk and responsibility always remains with the business.
  - Off-shoring, using outsource providers away from the centre of the business, introduces additional complications in security, political and environmental risk which may attract heightened interest from customers and regulators.
- **Changing the process** may provide an opportunity to continue with the business as far as the customers are concerned, but the deliverable is 'assembled' in a different way, usually by outsourcing all or part of the operation. For example a manufacturing company may become a distributor by importing and re-badging.
- **Ceasing or selling parts of the business** may be appropriate where the remaining business remains viable and may create space for recovery. This may also be an appropriate strategy for a Group of companies who are unwilling to budget for recovery capability in a marginal subsidiary. There are risks with this strategy if the reputation of the remaining business may

be tarnished by the failure of the ceased part.

- **Fortress** – for sites with unique manufacturing process or where the location is unique then a relocation strategy may not be possible. In this case all the effort must go into minimising specific threats in the hope that, if the worst happens, the uniqueness of the organisation will require its reinstatement however long this takes.
- **Asset restoration** services are provided by a range of specialist companies who can often minimise damage after fire and flood to papers, equipment and buildings. These firms may provide an advance registration service and advice, as well as being available on request post incident.
- **Insurance,** when properly arranged, can provide financial compensation for loss of assets, increased costs of working and protection for associated legal liabilities. However it may not provide cover for the full expense of an incident or damage including the loss of customers, impact of shareholder value or loss of reputation and brand image. The BCM should work closely with the Insurance Manager to dovetail insurance cover with BCM parameters,
  - An 'All Risks' type Policy will compensate for the assessed value of the damaged or lost physical assets and electronic records.
  - Business Interruption insurance may pay for either the "increased cost of working" during resumption or for 'loss of profits' over the disrupted period.
  - 'Keyman' insurance may provide a sum following the loss of named individuals from the business due to death, injury or resignation.
  - Liability insurance may provide protection for liabilities incurred including those associated with employees and third-party property and people.

Site resilience and specific threats

- **Monitoring systems** may provide prompt warning of utility failures, equipment failures and destructive threats
- **Uninterruptible Power Supply (UPS) and back-up generators** can protect buildings or specific equipment from power failures. They need to be maintained and tested regularly to ensure performance when required. There are also specialist recovery contracts that will supply portable generators either as a contracted service or on demand (subject to availability).
- **Sprinkler and Fire Suppression systems** are often advised for buildings with high loading of flammable materials or expensive equipment. Whilst water can put out fires effectively, it can cause considerable damage to papers and electronic equipment.
- **Cross-Training & Documentation** can provide some protection against loss or absence of key staff
- There are many other measures able to protect a site or pieces of equipment against specific threats identified in a risk analysis

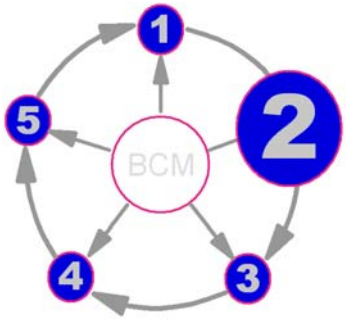
General considerations

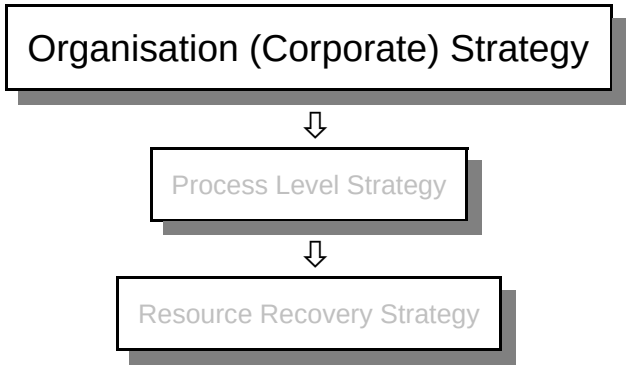
Continuation or restart capabilities need to be realistic. Physically moving staff and operations will take more time than expected and impact on the available working day. It is important to allow sufficient continuation/restart time into the expected Recovery Time Objectives (RTO) to ensure resumption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

It is usually the case that the faster the recovery requirement, the greater the cost of a solution

therefore, to minimise costs, it is important to ensure that an appropriate, but not excessively rapid, recovery strategy is chosen.

2.1 Organisation (Corporate) Strategy





Introduction

An organisation's Business Continuity Management Strategy works best when its vision, direction and parameters are given from the top of the organisation.

There should be a clear transition between each of the above BCM Strategies. There are dependencies between each strategy that must follow a natural progression from one to the other.

Precursors

The organisation-wide strategy must be adhere to the BCM Policy.

Purpose

The purpose of an Organisational (Corporate) Business Continuity Management Strategy is to provide a clearly defined and documented policy, framework and operational direction to ensure continuance of that organisation.

Concepts and Assumptions

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

Whilst it is self-evident that greater geographical separation decreases the likelihood of two sites being affected by the same incident, there is no 'minimum' or 'correct' distance for separation as the ability of world-wide infections and computer viruses to cause concurrent incidents demonstrates. However a few hundred metres is likely to provide little protection even in localised incidents because of the way that emergency services use cordons and the likely disruption to

transport. Some organisations can use their market or jurisdiction area to define the limit of their dispersion (see discussion of survivable incidents in the Introduction to Stage One), others may choose the pragmatic alternative of placing a relocation site within the limit of how far they judge their staff would travel (which may be about 1 hour away).

Syndication Ratios

- "Dedicated" work area where a subscriber has exclusive use of accommodation. This is generally used where a rapid RTO is required, for high value-generating functions, where specialist equipment is used or where the non-availability associated with syndicated space are judged unacceptable. An example would be dealing desks for an investment company.
- "Syndicated or Subscription" work area where a subscriber pays for the use of accommodation provided that it is not already in use by a prior invocation by another subscriber.
    - The general industry ratio is a maximum of between 40 & 25 to 1 i.e. each desk is sold a maximum of up to 40 times, but great care should be taken to understand who are the other customers potentially using each desk e.g. some suppliers provide client details by post code. The parameters acceptable to an organisation should be clearly defined within its BCM Resource Recovery Strategy and should not be left to individual contract negotiations.
    - At the current time there are two basis on which the available resources may be allocated by a recovery supplier to subscribers during a concurrent invocation:
        - First come, first served : The first subscriber to invoke the service gets their full allocation of resource, any remainder is available to subsequent subscribers
        - Equitable share : The available resources are allocated in proportion to the resources subscribed to.

Exclusion Zones (Third-party recovery sites)

The exclusion zone is the distance within which the recovery supplier will not resell the resources you have subscribed to another potential customer. The organisation's definition of exclusion zones should be clearly defined within the corporate BCM Strategy e.g. within the City of London a 800 metre exclusion zone (vehicle size bomb) is a minimum acceptable standard for this specific threat but may not be appropriate for other types of incident.

Resilience

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

- The addition of RAID technology to a computer increases ***machine-resilience*** (but only to hard-disc failures) and does nothing to protect against loss of that machine in a fire
- Duplication of power feeds to a site increases ***site-resilience*** to power interruptions but the site can still become unusable if the power failure affects both supplies
- Expanding the geographical dispersion and diversity of the organisations locations increases ***organisational-resilience***

Process

The process includes the following stages:

- Form a Business Continuity Management Strategy Team.
- Identify the Organisation's Business Strategy, its objectives, legal and regulatory requirements and understand how a Continuity Strategy will support these objectives.
- Review the scope, assumptions and findings of the Business Impact Analysis
- Generate outline strategy options for consideration.
- Provide executive management with the evaluation report to choose options, which they can determine based on the organisation's current and future business strategy and risk appetite.
- Ensure the agreed outline option is 'signed-off' by the executive management including the financial and resource provisions.
- Develop the detail of the agreed strategy for business processes and resource recovery.
- Implement an on-going process to ensure the Organisation's BCM Strategy planning is reviewed.

Methods and Techniques

The tools that could be used to develop an Organisation (Corporate) Business Continuity Management Strategy include:

- Strategy planning tools
- Benchmarking against appropriate national and international standards
- PEST Analysis (Political/ Environment/Social/Technical)
- Cost Benefit Analysis (including stakeholder, legislative and regulatory assessment)
- SWOT Analysis (Strengths/Weaknesses/Opportunities/Threats)
- Financial Planning and Management

Outcomes and Deliverables

The outcomes are:

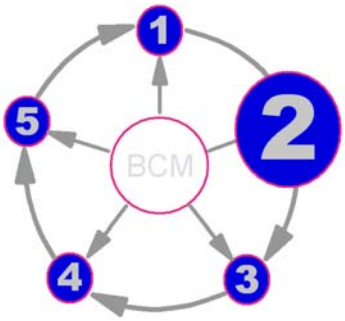
- A organisation-wide BCM Strategy based on the organisation's business strategy and risk appetite
- An operational BCM framework which supports the BCM Strategy.

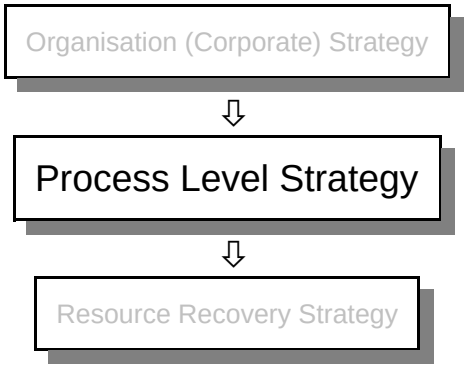
Review

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

- A Business Impact Assessment revision identifies changes in business critical processes and priorities.
- A significant change in one or more of the following: key technology, telecommunications, business risk appetite, accommodation, staffing, acquisition or merger, new products or services, service suppliers, regulatory or legislative requirements

2.2 Process Level Strategy





Introduction

A Business Impact Analysis will identify the priority of resumption of business critical processes and activities. At the Process Level Strategy the complexity of interdependencies on services, business processes, data and technologies needs to be analysed.

In determining the Process Level BCM Strategy, reference must be a clear transition between each of the above BCM Strategies. There are dependencies between each strategy that must follow a natural progression from one to the other.

Precursors

The Process Level BCM Strategies need to be developed within the context of the Organisation's overall BCM Strategy.

Purpose

The purpose of a Process Level Business Continuity Management Strategy is to provide a documented framework for the resumption for one or a number of business critical processes and activities.

Process

The process includes the following stages:

- Create an overall Process Level BCM Strategy within the parameters of the Corporate Recovery Strategy
- From the Business Impact Analysis and Risk Assessment identify business critical processes

and activities including their dependencies and any single points of failure.

- Using the results from the Business Impact Analysis note the Maximum Tolerable Outage (MTO).
- Decide on a Recovery Time Objective (RTO) for the process, which should (or course) be shorter than the MTO.
- If there is an existing resumption strategy conduct a 'Gap Analysis' to identify where existing performance is measured against the required performance.
- Identify appropriate strategy or strategies for each business critical process and activity and generate Process Level BCM Strategy options.
- Evaluate the cost benefit analysis for the Process Level BCM Strategy options with regard to optimise efficiency, to attain recovery time objectives and to ensure cost effectiveness.
- Provide executive management with a strategic evaluation, which they can determine based on the organisation's risk appetite.
- Ensure the agreed option is 'signed-off' by the executive management including the financial and resource provisions.
- Create Process Level Strategy implementation project and action plans. A Risk Assessment, if completed for that process, may suggest priority areas for implementation
- Implement projects to develop plans for Business processes.
- Implement an on-going process to ensure the Process Level BCM Strategy planning is reviewed.

Methods and Techniques

The tools available to develop a Process Level Business Continuity Management Strategy include:

- Results from the Business Impact Analysis and Risk Assessment
- PEST Analysis (Political/ Environment/Social/Technical)
- Cost Benefit Analysis
- End-to-End service and process mapping.
- Crisis Management planning

Outcomes and Deliverables

The outcomes and deliverables from a Process Level Business Continuity Management Strategy include:

- A documented Process Level BCM Strategy, agreed and 'signed-off' by the organisation's executive management.
- A project plan for implementing the agreed strategy.
- An agreed relationship with the organisation's Business Continuity Management process to develop a Process Level Business Continuity Plan (BCP) for one or a number of business

critical processes and activities.

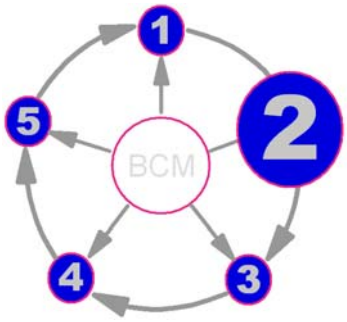
- A developed and agreed relationship in the organisation's Crisis Management process.
- Compliance with legal and/or regulatory requirements for a Business Continuity Plan.

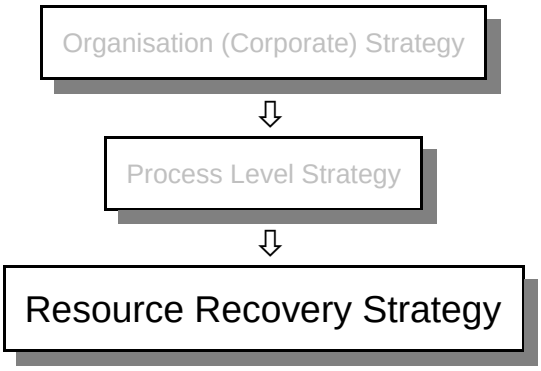
Review

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

- A Business Impact Assessment revision identifies changes in business critical processes and priorities.
- A significant change in the following: key technology, telecommunications, accommodation, staffing, acquisition or merger, new products or services, service suppliers, regulatory or legislative requirements any one of these businesses may cause a review of the Process Level BCM Strategies.

2.3 Resource Recovery Strategy





Introduction

This step provides the Resource Recovery BCM Strategy is directly linked to the Business Impact Analysis and must document and evaluate the factors for:

- Deployment of appropriate recovery resources across a number of business critical processes and activities.
- Work area requirements – staff ratio, priority of business processes, location (in-house or third party) and technology requirements

Precursors

The parameters for the Resource Recovery BCM Strategy will be derived from the timescales in the Process Level BCM Strategy and the resources identified in the Recovery Resource Analysis (RRA).

Purpose

The purpose of a Resource Recovery BCM Strategy is to co-ordinate and provide a predetermined level of resources within a Business Continuity Plan (BCP) to enable the implementation of the Organisation (Corporate) BCM Strategy and Process Level BCM Strategy.

Concepts and Assumptions

Availability of solutions

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

Process

This process includes the following stages:

- Aggregate Resource Recovery requirements from the Process Level BCM Strategies by classifying BCM solutions that can provide resources for the required resumption strategy
- Identify appropriate strategy or strategies for each business critical process and activity and generate Resource Recovery BCM Strategy options
- Evaluate the cost benefit analysis for each of the Resource Recovery BCM Strategy options to attain recovery time objectives and to ensure cost effectiveness.
- Provide executive management with a strategic evaluation, which they can determine based on the organisation's risk appetite.
- Ensure the agreed options are 'signed-off' by the executive management including the financial and resource provisions.
- Create Strategy implementation project and action plans
- Apply the agreed strategy to implement the project and action plans (including the development of Business Continuity Plans).
- Implement an on-going process to ensure the Resource Level BCM Strategy planning is reviewed.

Methods and Techniques

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

- Results from the Business Impact Analysis and Resource Recovery Analysis as refined by the Process Level Recovery Strategy
- Evaluation tools for purchasing services including value-for-money and contractual terms assessment
- Alternative site working strategies for : work areas, IT facilities, telecommunications

- Provision for : off-site data storage, damage assessment and salvage operations
- Measures to manage loss of staff
- Cost Benefit Analysis

Outcomes and Deliverables

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

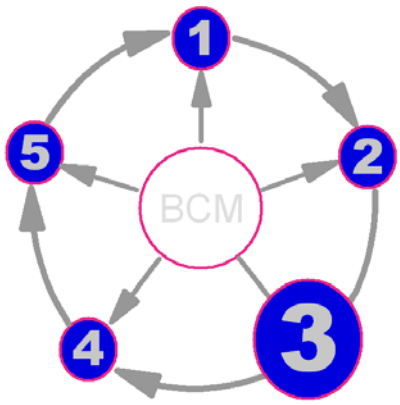
- A set of recovery resources and services which can be deployed under the control of the Business Continuity Plan (BCP) that provides for the restoration of acceptable functionality for business processes
  - within their Recovery Time (RTO)
  - with data recovered to within their Recovery Point Objectives (RPO).

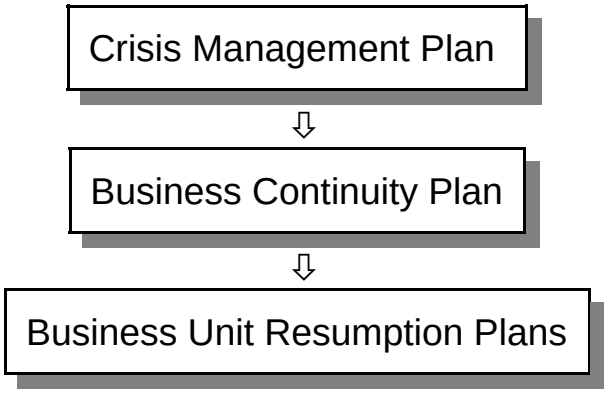
Review

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

- Changes required by Process Recovery Requirements
- A significant change in accommodation, staffing or available technology that may provide alternative resumption strategies
- A change in the availability of recovery services in the vicinity such as closure, merger or opening of a facility

Stage 3 : Developing a BCM Response



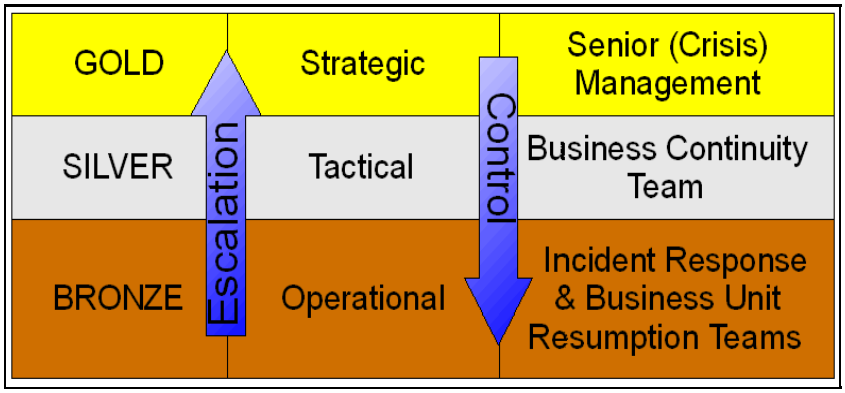


Introduction

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

The actions outlined in the plan are not intended to cover every eventually as, by their nature, all incidents are different. Likewise the predefined procedures may need to be adapted with flexibility and initiative to the specific event that has occurred and the opportunities it may have opened up. If the event falls outside the scope of the assumptions on which the Business Continuity Plan was based then the situation should be escalated to those responsible for implementing the Crisis Management Plan.

One model of incident response, borrowed from the UK Emergency Services, shows three tiers of incident response often referred to as Gold, Silver and Bronze.



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

Tactical : Business Continuity Plan: addresses business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed. They are based upon the agreed Business Continuity Strategies and provide procedures and processes for both the

business continuity and resource recovery teams. In particular the plans allocate roles and their accountability, responsibility and authority. The plans must also detail the interfaces and the principles for dealing with a number of external players in the response such as recovery services suppliers and emergency services.

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

Timeline

In a destructive incident the three types of plans will address different issues during the various phases of the event. For example:

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

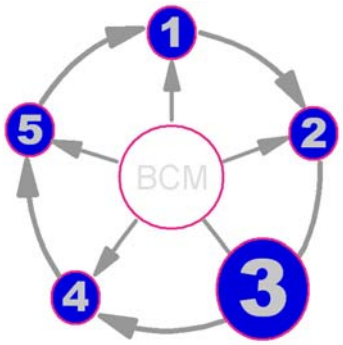
Scaleability

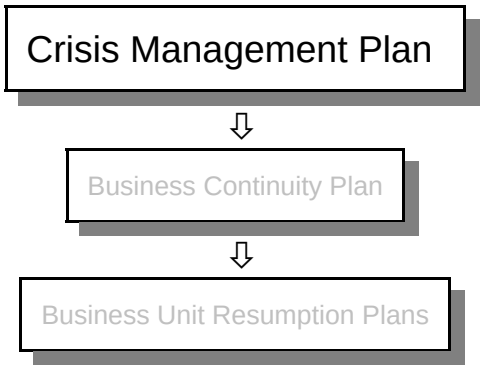
Whilst the three levels provide a suitable model for a medium sized organisation with a single site a smaller organisation may have a single 'hands-on' management group with both tactical and strategic responsibilities. However it is still important that this group addresses the strategic issues despite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

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

- A response team at each site with a central Business Continuity 'flying squad'
- A Business Continuity team at each major site with a central Crisis Management Team
- Both BCM and CMT at a national level with limited involvement from the International Board unless global reputation is threatened

3.1 Crisis Management Plan





Introduction

Case studies of major incidents (Knight and Pretty) suggest that effective and timely management of a crisis is the significant factor in protecting an organisation's brand from financial and reputation damage.

Precursors

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

Purpose

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

Concepts and Assumptions

The terms used in these Guidelines for the various plans are not universally applied, in particular the term crisis team may be applied to what others would call an incident response team. It is important that an organisation chooses names that fit into its culture and structure, but that the roles described here are covered.

Process

The key steps in developing a Crisis Management Plan include:

- Appoint an owner for the Crisis Management Plan on the Executive
- Define the objectives and scope of the plan
- Develop and approve a Crisis Management plan development process and programme
- If no plan exists it may be useful to run an exercise with the CMT but exerting minimal pressure, so that the many requirements of a plan become apparent (including the need for a plan)

- Create a crisis management planning team to develop the plan
- Agree the responsibilities of the Crisis Management Team and their relationship with other plans (an example list of responsibilities is in the appendix)
- Decide the structure, format, components and content of the plan
- Determine the strategies, such as alternative locations, on which the plan is based
- Gather information to populate the plan
- Nominate individuals to fulfil roles within the plan
- Draft the plan
- Circulate the draft of the plan for consultation and review
- Gather feedback from the consultation
- Amend plan as appropriate
- Agree and validate the plan, for example by using it in an exercise
- Repeat process for the Crisis Communications Plan (if separate)
- Agree a programme of ongoing exercising and maintenance of the plan to ensure it remains current

Methods and Techniques.

Building the CM Plan

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

- Stakeholder analysis
- Scenario planning
- Checklist(s)
- Workshops
- CMP Templates for distribution to assist implementation of standard procedures in an international organisation

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

CMP Contents

As, by their nature, all crises are different the Crisis Management Plan is a set of components and resources which may be useful. The contents will also depend on the nature and complexity of the organisation.

The Crisis Management Plan should be modular in design so that single sections can be supplied to individuals and/or teams on a need-to-know basis. It is suggested that the different sections are

printed on different coloured paper to provide ease of use at the time of a crisis.

A sample table of contents of a Crisis Management Plan is in the Appendix of Sample Documents.

Crisis Communications Plan

Consider in advance:

- What crises could hit us? (A Risk Assessment may be appropriate)
- Who are the Audiences?
- How do we Communicate with them?
- What are the Messages?
- Who will form the Crisis Team?
- What are the Resources and Facilities?
- Are the crisis team and spokespeople Trained?
- Does it Work?
- What Crisis Manual do we need?
- Have we built lines of communication with our audiences?

When a crisis or business discontinuity gets into the public domain, effective communication will play a key role in rescuing and maintaining an organisation's most valuable asset - its reputation.

If faced with a crisis consider:

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

Further details on crisis communications are in the Appendix of Sample Documents

Outcomes and Deliverables

The outcomes of the Crisis Management Planning process include:

- A Crisis Management Plan that can support the role of the organisation’s Crisis Management Team during a crisis event

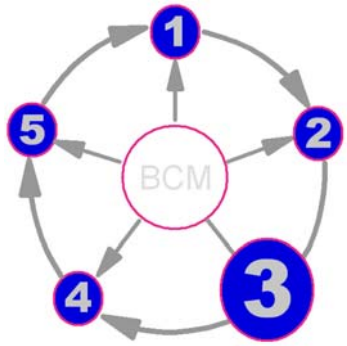
- A Crisis Communications Plan that can manage the media and stakeholder communication during a crisis
- Demonstration of preparation for effective crisis management to the media, markets, customers, stakeholders and regulators
- Compliance with legal requirements
- Compliance with regulatory requirements

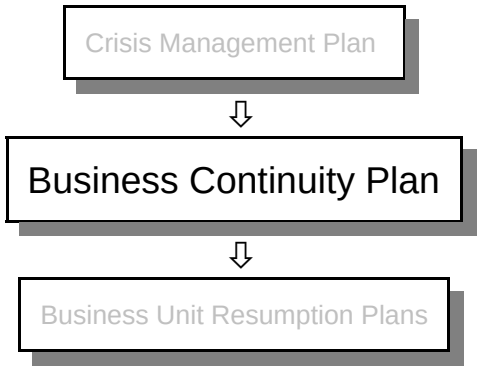
Review

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

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

3.2 Business Continuity Plans





Introduction

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

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

Precursors

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

Purpose

The purpose of a Business Continuity Plan(s) is to provide a documented framework and process to

enable the organisations to resume all of its business processes (or, as a minimum those required most rapidly) within their MTO. A Business Continuity Plan on its own does not demonstrate a BCM competence or capability; but the presence of a current plan which has been produced by the organisation does suggest an effective capability

Concepts and Assumptions

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

Process

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

- Appoint an owner for the BC Plan (or each plan for multiple sites)
- Define the objectives and scope of the plan with reference to the organisational strategy and BCM Policy
- Develop and approve a planning process and timetable programme
- Create a planning team to carry out the plan development
- Decide the structure, format, components and content of the plan
- Determine the strategies which the plan will document and what will be documented in other plans
- Determine the circumstances that are beyond the scope of the BCP
- Gather information to populate the plan
- Draft the plan
- Circulate the draft of the plan for consultation and review
- Gather feedback from consultation process
- Amend the plan as appropriate.
- Test the plan using a desktop exercise
- Schedule ongoing exercising and maintenance of the plan to establish it remains current

Methods and Techniques

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

A variety of software products is available to assist in building and maintaining a Business Continuity Plan however it is not essential. Using normal office software (Word processor and spreadsheet) may suffice and is more inclusive of all staff since its use does not require special

training. Customised software can however provide significant benefits in the areas of plan maintenance and referential integrity.

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

An example showing the standard components of a Business Continuity Plan is included in the Appendix of Sample Documents.

Outcomes and Deliverables

The deliverables of the Business Continuity Management planning process include:

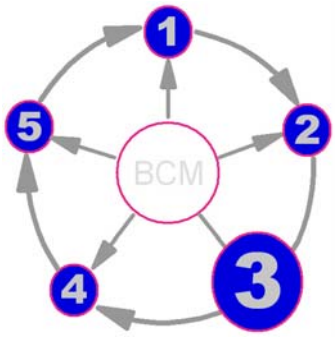
- A Business Continuity Plan which should be 'signed-off' by the Executive
- A framework within which Business Unit plans (next section) can operate

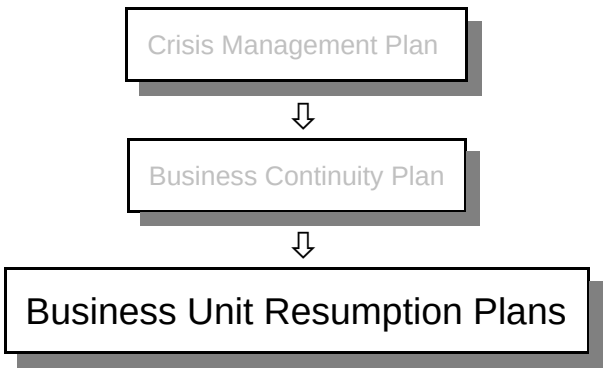
Review

Some information within a Business Continuity Plans such as contact details will require monthly or quarterly review. Other information should be formally reviewed annually and tested through exercising. Other triggers leading to a review are:

- A significant change in the technology and/or telecommunications
- There is a major business process change
- A significant change in staff
- A change in the supplier of BCM solutions

3.3 Business Unit Resumption Plans





Introduction

The Business Unit Resumption Plans provide the Operational Response to the incident of each department of the organisation. Examples of Business Unit plans are:

- An incident response team usually lead by a Facilities department who deal with the specific incident and its physical impact (if any)

- A Human Resources response to welfare issues in an incident
- A business department plan to resume its functions within a predefined timescale
- An IT department's logistical response to the loss and subsequent resumption of IT services to the business

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

Precursors

Because of the many links between the BC Plan and those of the Business Units, the BC Plan should be written, at least in outline, before these BU plans.

Purpose

The purpose of the Business Unit Resumption plan is to structure the response of each department to an interruption.

Concepts and Assumptions

Process

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

- Appoint a person to be responsible for development of the plans overall and a representative within each business unit to develop their plan
- Define the objective and scope of the plans
- Develop a planning process and timetabled programme. Where possible, begin with the plans for the most urgent functions
- Determine the overall BCM strategies on which the plan is based.
- Decide the structure, format, components and content of the plans
- Develop an outline or template plan to encourage standardisation of documentation but allow individual variations where this is appropriate
- Ensure that BUs nominate individuals to fulfil roles within their plans
- Manage and mentor the development of plans within the BUs
- Circulate the draft of the plan for consultation, review and challenge within and, where necessary outside, the department
- Gather feedback from consultation
- Amend plan as appropriate
- Validate the plan through a unit test
- Consolidate the BU plans and review for consistency

- Document connections with the BC Plan and between Unit plans
- Conduct a resource requirements analysis across all plans to define resource requirements for support functions

Methods and Techniques

The methods, tools and techniques to develop a Business Unit Resumption Plan include:

- Interviews (structured and unstructured).
- Checklists and templates
- Workshops

Specific Business Unit plans may include the following:

Facilities (Incident Response Team)

- Building Evacuation and Invacuation plans
- Response to Bomb Threat and similar scenarios
- Evacuation points (including alternate or off-site)
- Dispersal of staff and visitors
- Salvage Resources and contracted assistance
- Escalation circumstances

Human Resources

- Welfare issues
- Health and Safety legal liabilities
- Procedure for accounting for staff
- Procedure for contacting staff
- Counselling and rehabilitation resources

Operational Business Unit Resumption

- Escalation criteria for invoking Business Continuity Response (problem is out of 'comfort zone' for business unit)
- Escalation procedure to Business Continuity Team (BCT)
- Initial contact from BCT
- Contacting team members
- Resumption Plan for each process
    - Staff numbers
    - Key contacts
    - Consumables

Outcomes and Deliverables

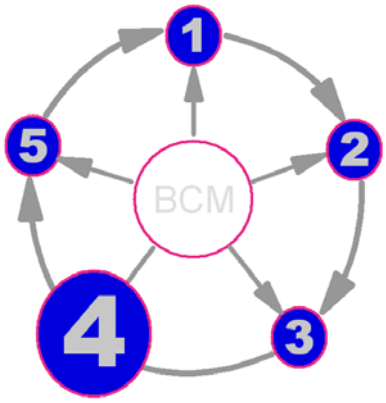
The outcomes of the Business Unit Resumption Plan include:

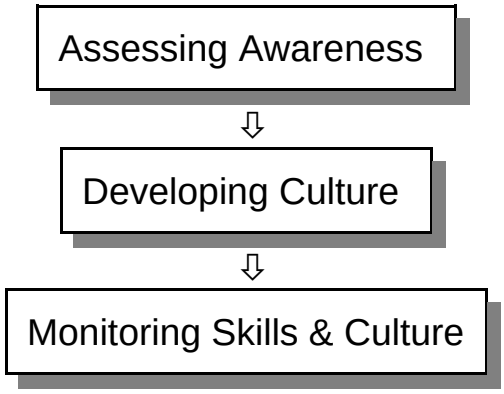
- A documented Business Unit Resumption Plan for each department
- Criteria for BU to escalate issue to BCT
- Clearly defined BCM roles within the department

Review

Business Unit plans should be reviewed if there is a major change in the business process or technology within that unit.

Stage 4: Developing a BCM Culture





Introduction

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

The main techniques for developing a sustainable BCM culture within an organisation include:

1. Assessing the current level of awareness of, and commitment to, BCM against the desired level; thus identifying the 'training gap' that exists between the two

2. Designing and delivering a campaign to create corporate awareness and develop the skills, knowledge and commitment required to ensure successful Business Continuity Management.

3. Checking that the awareness campaign has achieved the desired results, and monitoring BCM awareness in the longer term

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

Critical factors for success include:

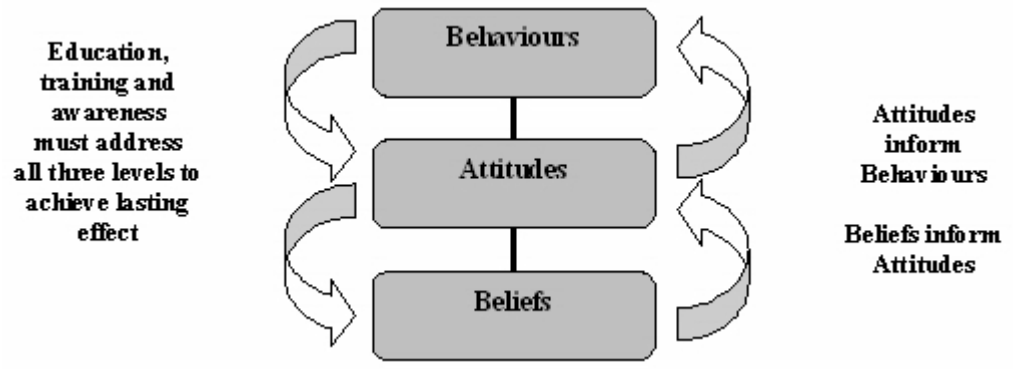
- Visible and continued support by senior management. This must include adequate budget to support the awareness campaign over time. It is also important to gain commitment from managers and operational staff who are required to implement Business Continuity Management.
- Consultation, with everyone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

The awareness campaign and its messages should be tailored to target audiences. These audiences

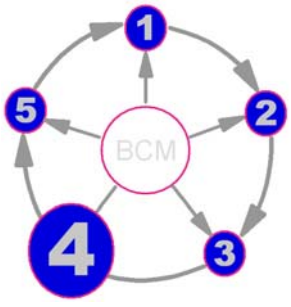
are both internal, for example BCM practitioners and general staff – and external, for example key stakeholders and third parties that are dependent on (or may adversely affect) the organisation's own business continuity management effort. External awareness is particularly important where BCM operates in an outsourced environment.

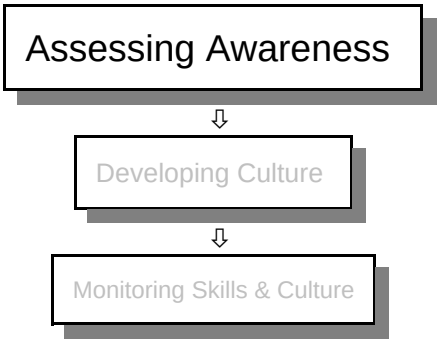
Organisational culture is manifested in shared values, operating norms, styles and patterns of behaviour. It is frequently described as 'the way we do things around here' or 'what you have to do to get on'.

Experience has shown that behavioural change initiatives fail to attract lasting commitment unless attitudes and beliefs are also engaged. In order to really change behaviours, it is necessary to influence the attitudes. In order to influence attitudes, it is necessary to develop and establish beliefs. Thus, achieving cultural change can be a subtle and lengthy process.



4.1 Assessing the level Of BCM Awareness





Introduction

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

Precursors

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

Purpose

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

Concepts and Assumptions

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

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

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

Process

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

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

Methods and Techniques

1 : Establishing the current level of awareness of BCM

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

Sources should include:

- **Documentation:** including corporate policy statements and procedures, incident and crisis response reports, accounts of previous BCM tests and exercises, relevant IT system and business metrics
- **People Feedback:** including interviews with senior management and business managers, focus

groups with practitioners and end-users

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

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

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

- Enhanced working practices that support BCM
- A better understanding of, and material support for, BCM issues by staff generally
- A higher BCM profile in corporate decision-making, policy and culture

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

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

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

Outcomes and Deliverables

The outcomes from the awareness assessment should include:

- A statement of the current level of awareness and effectiveness of staff to support BCM
- A statement of the desired level of awareness and how this will be measured
- A definition of the Training Gap, including BCM subjects which require greater awareness, staff attitudes to BCM - since this will help define the overall message of the awareness

campaign - and the level(s) of competence found in each target group.

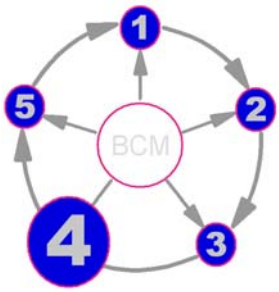
Review

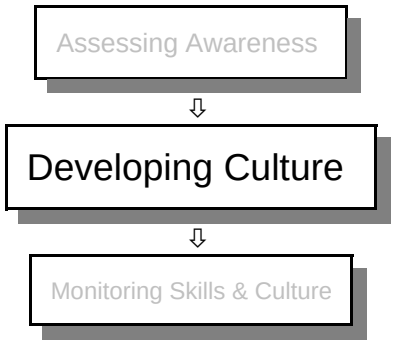
The awareness assessment should be carried out at the start of the awareness campaign, again following the main thrust of the campaign, and periodically thereafter as a monitoring capability.

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

- Organisational business processes that affect BCM priorities
- Legislation affecting BCM requirements
- The BCM risks including security threats and vulnerabilities and other business-related risks
- Corporate and client/partner requirements for the availability of information and services, including accepted industry Best Practice e.g. PAS56 and ISO17799

4.2 Developing a BCM Culture





Introduction

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

- Training & Awareness Design
- Training & Awareness Delivery Planning
- Training & Awareness Delivery

Precursors

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

Purpose

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

Concepts and Assumptions

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

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

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

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

Process

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

- Training & Awareness Design
- Training & Awareness Delivery Planning
- Training & Awareness Delivery

Training & Awareness Design

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

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

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

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

Training & Awareness Delivery Planning

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

drive.

Key activities in this task should include:

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

Training & Awareness Delivery

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

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

Methods and Techniques

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

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

Information resources:

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

Training resources:

- External approved training courses
- Formal academic educational programmes
- BCI Regional Forums and working groups
- Industry sector working groups

- Certification bodies
- Internal training, including specific induction and refresher courses
- Distance learning (CBT, video, reading)
- Certification bodies
- BCM and Crisis Management exercises (internal or external)

Awareness resources:

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

Outcomes and Deliverables

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

The outcomes of the campaign may include:

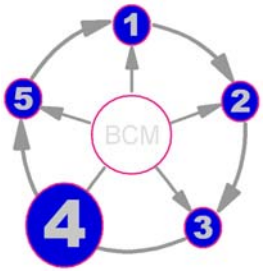
- Higher general awareness of the need for BCM
- Create awareness of BCM risks to the organisation and of business priorities
- Identification of an acceptable approach to BCM which can be integrated into working practices
- Improved effectiveness in conducting specific BCM tasks
- More effective responses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

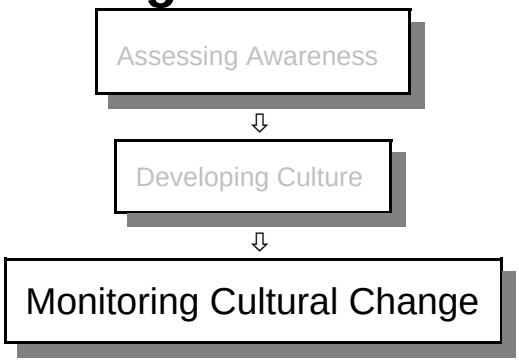
Review

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

- Organisational business activities that affect BCM priorities
- Legislation affecting BCM requirements
- BCM risks, including security threats and vulnerabilities and other business-related risks
- Corporate and client/partner requirements for the availability of information and services, including accepted industry Best Practice e.g. PAS56 and ISO17799

4.3 Monitoring Cultural Change





Introduction

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

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

Precursors

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

Purpose

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

Concepts and Assumptions

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

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

may be relevant for BCM culture generally.

Process

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

Methods and Techniques

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

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

Specifically, the evaluation of training courses may include discussions, quizzes or short examinations during the course to check and align teaching 'in flight'. Course Evaluation Forms may be used to improve continuously the course structure and content. Evaluation of a course should be based on a number of runs, rather than a single instance.

Outcomes and Deliverables

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

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

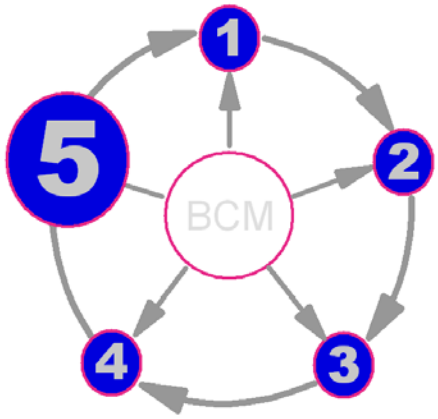
- Identification of further education, training and awareness requirements
- Identification of professional development opportunities for BCM practitioners
- Improvements in working practices

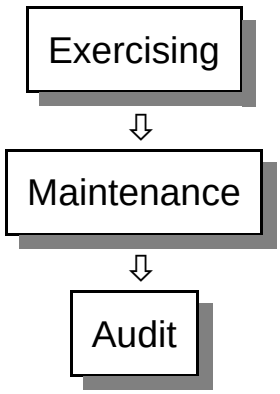
Review

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

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

Stage 5 : Exercising, Maintenance and Audit





Introduction

Exercising

A Business Continuity Management (BCM) capability cannot be considered reliable until it has been exercised.

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

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

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

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

Maintenance

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

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

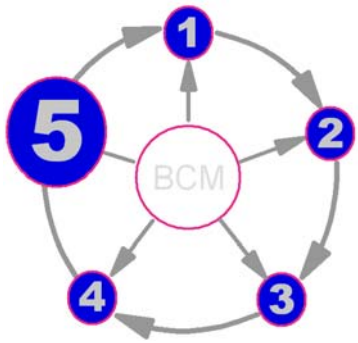
Audit

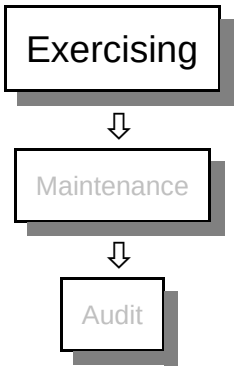
The BCM Audit process ensures that an organisation has an effective Business Continuity capability. Audit has five key functions:

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

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

5.1 Exercising





Introduction

The development a BCM capability is achieved through a structured exercising programme, to be successful an exercising programme must begin simply and escalate gradually.

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

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

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

opportunities for improvement rather than criticism.

Precursors

Not understanding how the plan would function if it were called into action is a key driver for initiating testing activities.

Purpose

The purpose of exercising is:

- To evaluate the organisation's BCM current competence.
- To identify areas for improvement or missing information
- To highlight assumptions which need to be questioned
- To provide information and instil confidence in exercise participants
- To develop team work
- To raise awareness of Business Continuity throughout the organisation by publicising the exercise.
- To test the effectiveness and timeliness of restoration procedures at the end of the exercise.

Concepts and Assumptions

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

Stringency

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

Realism

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

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

Minimal Exposure

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

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

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

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

Process

A technical test may include the following steps:

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

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

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

recommendations.

- Prepare an open-issues report during and immediately following the test.
- Circulate reports to participants and senior management
- Circulate report to participants and senior management
- Create an action plan to implement post exercise report recommendations i.e. update the strategy and plan as approved, review exercising schedule for further exercising to prove the efficacy of the changes.

Methods and Techniques

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

Type	Process	Participants	Frequency	Complexity
Desk Check	Review and Challenge the contents of the plan.	• Author of plan • Independent checker	**High**	**Low**
Walkthrough Plan and/or Infrastructure	Extended Desk Check to check interaction and the roles of participants	• Author of plan • Main participants	^	^
Simulation	Incorporates associated plans: • Business • Site/Buildings • Communication • Public Relations • ITDR BCM Resource Recovery Suppliers	• Main Participants • Facilitator • Observers • Co-ordinators • Umpires	▪	▪
Functions	Moves to and recreates one or a number of business functions at an alternative pre-planned site.	• Employees and staff in specific business area • Facilitator • Co-ordinators • Observers • BC Resource recovery Providers	▪	▪
Full Plan	Close down of entire site/building and relocation of work	• Staff required for recovery activities included in the BC Plans. • Facilitator • Co-ordinators • Umpires • Observers • BC Resource Recovery Providers	▪ V **Low**	▪ V **High**

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

Participants

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

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

Outcomes and Deliverables

The outcomes of the BCM exercising process include:

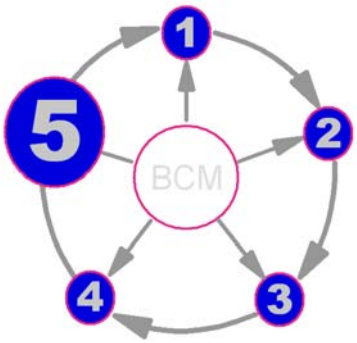
- Validation that the Business Continuity and strategies are effective
- Familiarity of team members and staff are familiar with their roles, accountability, responsibilities and authority in response to an incident.
- Testing of the technical, logistical, administration aspects of the Business Continuity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

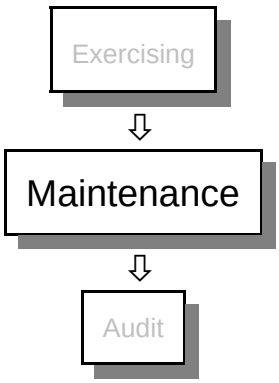
Review

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

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

5.2 Maintenance





Introduction

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

Precursors

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

Purpose

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

Concepts and Assumptions

Process

- Review internal changes to (for example):
  - Business processes
  - Technology
  - Staff

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

- Review and challenging the assumptions made in the BIA about the environment in which the organisation operates to determine whether the time imperatives have changed since the last review
- Review the adequacy and availability of external services that might be required by an

organisation in times of difficulty such as asset restoration, recovery sites and subcontracts

- Review the Business Continuity arrangements of suppliers of time-critical components to the business
- Assess whether changes and amendments create a training, awareness and/ or communication need.
- Deliver appropriate training, awareness and/ or communication where applicable.
- Distribute updated, amended, changed BCM policy, strategies, solutions, processes and plans to key stakeholders under the formal change (version) control process.

Methods and Techniques

- Each plan owner is responsible for updating the team's BC plans and dynamic data such as staff out-of-hours contact numbers, team tasks, notification and supplier contact details, contingency-box contents etc.
- Plan sections are updated at frequencies ranging from monthly to annually, in accordance with the schedule laid down in the BC Plan Maintenance Chapter/Section. The appropriate update months are also specified in the BC Plan Maintenance Chapter/Section.
- 'Date of last update' is clearly displayed at the beginning of each BC plan Chapter/Section to provide an effective audit trail.

Outcomes and Deliverables

The outcomes from the BC maintenance process include:

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

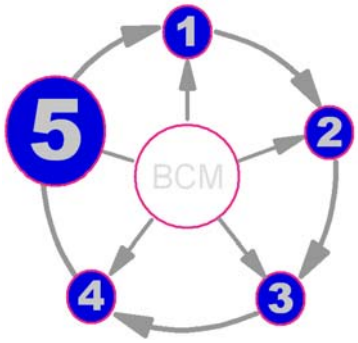
Review

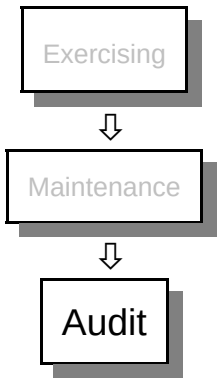
The frequency of a BCM Maintenance Programme is dependent upon the nature, scale and pace of business change.

Maintenance is likely to be required when:

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

5.3 Audit





Introduction

An audit function is one of impartial review against defined standards and policies and to provide remedial recommendations. However the nature of BCM may require a different audit approach because standards are constantly evolving.

Precursors

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

Purpose

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

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

Concepts and assumptions

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

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

- Regulatory requirements e.g. Financial Services Authority, The DTI
- Legislative requirements.
- Industry 'Good Practice' guidelines.
- Industry standards e.g. ISO 17799 (IT Security).

Process

The BCM audit, like BC planning, implementation and maintenance is concerned with a complex

process and requires interaction with a wide range of managerial and operational roles from both a business and technical perspective.

The BCM audit process includes:

- A BCM audit plan - which should include:
  - Identification of the type of audit to be carried out e.g. compliance, project management/control, feasibility study, due diligence or investigative.
  - Identification of the audit objectives i.e. outcomes and deliverables. The audit objectives may in part be driven and governed or restricted by legal or regulatory requirements. This includes key issues of high priority.
  - Identification of the standard audit framework (where appropriate) to be used e.g. PAS 56. The audit framework may be governed or restricted by legal or regulatory requirements.
  - Definition of the audit scope:
    - Determine the corporate governance, compliance or other issues to be audited.
    - Determine the area/department/site of the organisation to be audited.
  - Definition of the audit approach:
    - The auditing activities that will be undertaken e.g. questionnaires/face-to-face interview/document review/solution review.
    - Activity timetable and due dates
  - Identification of the audit evaluation criteria (standards).
  - Determine the requirement for specific subject expertise or third party assistance to conduct the audit.
- Review and information gathering via the BCM audit activities.
- Compile and summarise interview notes, questionnaires and other sources.
- Identify gaps in content and level of information gathered and conduct further or follow up interviews as appropriate.
- Obtain and compare relevant documentation e.g. Business Impact Analysis with interview data and other sources e.g. walkthrough, physical inspection, sampling).
- Refer to secondary sources e.g. standards, regulations, 'good practice' guidelines to validate preliminary findings.
- Form an opinion that should reflect both the interests of the audit sponsor and the 'yardstick' set by external sources e.g. regulatory, legal, industry standard.
  - Assign a risk weighting to individual audit item to distinguish between critical, high, medium and low risk findings.
  - Define criteria for rating factual findings by using a clearly differentiated categorised predefined rating level.
- Provide a draft audit opinion report for discussion with key stakeholders.
- Provide an agreed audit opinion report incorporating recommendations as well as auditee responses where differences of opinion persist.
- Provide an agreed remedial action plan including timescales to implement the agreed recommendations of the audit report. This should also form a key element of the BCM Maintenance Programme.

- Provide a monitoring process (in addition to the BCM Maintenance Programme) to ensure that the audit action plan to address material deficiencies is implemented within the agreed timescale.

The BCM Assurance process includes:

- Define role accountabilities, responsibilities and authority
- Define Key Performance Indicators (KPIs) – Objectives, measurement targets and standards
- Define success factors
- Incorporate Key Performance Indicators in internal and external contract terms and annual appraisal
- Evaluate and review performance against Key Performance Indicators, objectives, targets and defined industry standards.
- Provide remedial action plan.

Methods and Techniques

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

Audit

Self-auditing, or 'Performance Monitoring' may be carried out more frequently, by the owners of the BC plans themselves. The BC Plans are measured against specified performance levels, in topics such as:

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

BCM Assurance

- Creation of a BCM Budget for implementation and maintenance.
- Budgetary control.
- Document analysis and review.
- Self assessment assurance scorecard.
- Interviews.

Outcomes and Deliverables

The outcomes of a BCM audit include:

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

Review

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

