



BUSINESS CONTINUITY INSTITUTE

GOOD PRACTICE GUIDELINES 2007

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

SECTION 5 EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS

ABOUT THIS GUIDE

1. Introduction

The BCI published its first Good Practice Guidelines in 2002. This played a significant part in the development of the British Standards Institution's (BSI) Publicly Available Specification for Business Continuity Management (PAS 56). GPG05 was issued followed by an extensive rewrite in to take into account the latest thinking in BCM internationally and to recognise increasing maturity in BCM practice across all sectors, public and private.

This guide to implementation of Business Continuity Management (BCM) has been prepared to support the launch of BS 25999-1 A Code of Practice for Business Continuity Management by the British Standards Institution. It can be viewed as implementation guide to BS25999 and as a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner.

There is a close relationship between the structure of this GPG and BS 25999-1 because the BCI GPG has always been a key component of BSI initiatives in the BCM field. A further revision is envisaged once BS 25999-2 is published since this will identify a management framework and which elements become mandatory.

However as a global institute, The BCI needs to reflect good practice across the world. BS25999 offers a comprehensive view of the subject but there are other standards in place with which many BCI professional members need to understand. As such the GPG07 is also designed to cover the main requirements of NFPA1600 (US and Canada) HB221 (Australia), APS 232 (Australia) and FSA (UK).

In no cases, however, must the GPG be seen as a replacement for those standards or as a guarantee of compliance with those standards.

2. Format of this Guide

The Guide has been prepared in 6 sections, which are in line with the earlier versions of the Guide and also with BS25999 nomenclature.

Section 1 consists of the introductory information plus **BCM Policy and Programme Management**

Section 2 is **Understanding the Organisation**

Section 3 is **Determining BCM Strategy**

Section 4 is **Developing and Implementing BCM Response**

Section 5 is Exercising, Maintaining & Reviewing BCM arrangements

Section 6 is **Embedding BCM in the Organisation's Culture**

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

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

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

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

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

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

GUIDELINES STAGE 5:
EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS

COMPONENTS

5.0 EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS	4
5.1 EXERCISE PROGRAMME	6
5.2 EXERCISING BCM ARRANGEMENTS	8
5.3 MAINTAINING BCM ARRANGEMENTS	12
5.4 REVIEWING BCM ARRANGEMENTS	14
KEY BCM INDICATORS	Error! Bookmark not defined.

5.0 EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9

1. General Principles

Exercising

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

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

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

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

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

Maintenance

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

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

Review

There are several ways to review a BCM programme including:

- Internal audit
- External audit
- Self-assessment

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

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

The Audit process can be undertaken by an organisation's Internal Audit function, an External

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

5.1 EXERCISE PROGRAMME

Ref: BS 25999-1 Section 9.2

1. Introduction

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

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

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

2. Precursors

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

3. Purpose

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

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

4. Concepts and Assumptions

Outsourced activities

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

5. Process

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

Recovery processes

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

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

6. Methods and Techniques

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

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

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

7. Outcomes and Deliverables

The outcomes of the BCM exercising programme process include:

- A timetable for an exercise programme

8. Review

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

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

5.2 EXERCISING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.3

1. Introduction

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

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

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

2. Precursors

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

3. Purpose

The purpose of exercising is to:

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

4. Concepts and Assumptions

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

Stringency

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

Realism

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

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

Minimal Exposure

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

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

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

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

5. Process

A technical test may include the following steps:

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

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

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

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

6. Methods and Techniques

Participants

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

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

7. Outcomes and Deliverables

The outcomes of the BCM exercising process include:

- Validation that the Business Continuity 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

8. Review

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

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

5.3 MAINTAINING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.4

1. Introduction

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

2. Precursors

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

3. Purpose

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

4. Concepts and Assumptions

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

5. Process

Review internal changes to

- Business processes
- Technology
- Staff

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

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

6. Methods and Techniques

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

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

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

7. Outcomes and Deliverables

The outcomes from the BC maintenance process include:

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

8. Review

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

Maintenance is likely to be required when:

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

5.4 REVIEWING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.5

1. Introduction

The review activity includes

- Audit, both internal and external
- self assessment

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

2. Precursors

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

3. Purpose

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

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

4. Concepts and assumptions

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

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

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

5. Process

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

The BCM audit process includes:

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

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

The BCM Assurance process includes:

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

6. Methods and Techniques

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

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

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

Qualitative assessment may come from:

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

7. Outcomes and Deliverables

The outcomes of a BCM audit include:

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

An outcome of a self-assessment process may be:

- Improvement in the management of the BCM programme

8. Review

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

Section 6 of the Good Practice Guidelines examines:
Embedding BCM in the Organisation's Culture