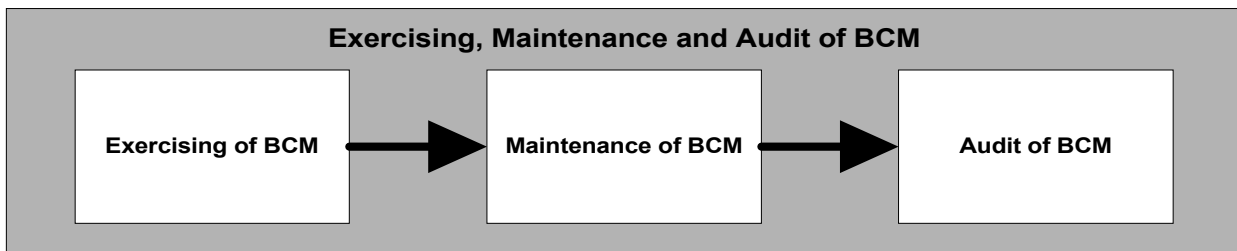


Stage 5 : Exercising, Maintenance and Audit



Introduction.

Exercising.

An effective fit-for-purpose Business Continuity Management competence and capability cannot be considered reliable until it has been exercised and proven as workable, especially since false confidence may be placed in its integrity. Consequently, exercising the Business Continuity Plan assumes considerable importance in establishing the Business Continuity Management competence and capability of an organisation.

Exercising can take various forms, from a technical test of the communications system, a desktop walk-through to a full live exercise. No matter how well designed and thought-out a Business Continuity Management Strategy or Business Continuity Plan; a series of robust and realistic exercises will identify issues that require attention. In addition to suggesting a perfect plan flawless exercising also suggests the adequacy and realism of exercising needs to be challenged and reviewed.

Time and resources spent exercising Business Continuity Management Strategies and Business Continuity Plans are crucial parts of Business Continuity Management as they enable competence, instil confidence and knowledge that lead to a fit-for-purpose Business Continuity Management capability that is essential at times of crisis and uncertainty.

The degree of continuous advancement in business automation together with its technological coupling and complexity is a key determinant and driver of the level of resource necessary to support exercising, testing and rehearsing.

Highly automated systems require 'High Reliability' and should be designed to test routinely in the course of normal operations. These tests may be invisible to customers and operations staff alike. Testing such systems may entail switching off items of equipment to monitor for any service effects or transferring service to another location without any or very limited service impact. There should be no sense of crisis or diverting of resource to testing. It should all be catered for in the design of business as usual.

Less advanced systems will require significant diverting of production resources to rehearse separate standalone recovery processes and locations with full use of crisis management, IT disaster recovery, and business resumption plans and teams.

The traditional approach of over emphasis on the exercising of information technology systems (IT) has now been recognised as a too narrowly focused Business Continuity Management approach. The key element of Business Continuity Management has now been realised as the role of people and their resilience in skills, knowledge, management and decision making. The need for the rehearsal of roles (people) and their place within the organisation hierarchy is fully recognised as a critical element within an organisation's exercising programme.

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 Business Continuity Management capability (including solutions and plans) continues to reflect the nature, scale and complexity of the organisation it supports, it must be fit-for-purpose, up-to-date, accurate, complete, exercised and understood by all relevant stakeholders and participants.

In essence, to retain its effectiveness, it must be vigorously maintained. In particular it ensures the continuity of competent and capable key people who clearly understand their Business Continuity Management roles and responsibilities to implement the Business Continuity Management Strategies and Business Continuity Plans in the event of an incident occurring.

Business Continuity Management 'Good Practice' makes no distinction between internal or outsourced operations; while a service or function may be outsourced, the risk accountability cannot. Consequently, the supplier(s) of Mission Critical Activities, their dependencies (intra-organisation or outsourced providers) and/or Resource Recovery Specialist e.g. external work area providers, must also undertake maintenance activities to assure their Business Continuity Management competence and capability based on their supplier 'due diligence' requirements.

A clearly defined and documented Business Continuity Management Maintenance Programme and processes must be established; further, effective documented change control procedures implemented to ensure all relevant stakeholders have the current and relevant parts of the Business Continuity Plan. Business Continuity Management maintenance activities should be agreed and proactively supported by senior management, and undertaken at all the levels at which it is managed within an organisation.

Audit.

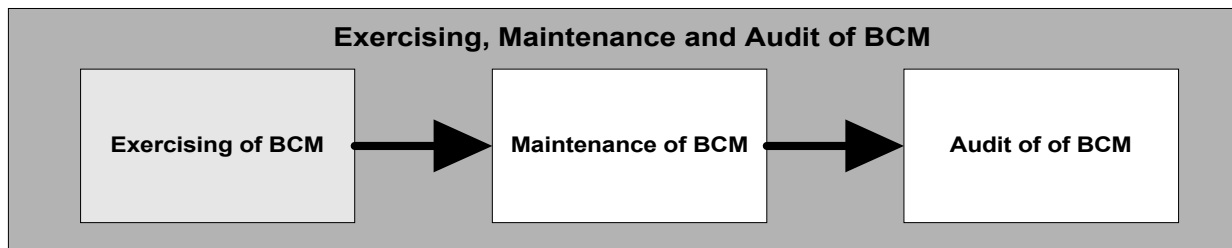
The Business Continuity Management Audit process also plays a key role in ensuring that an organisation has a robust, effective and fit-for-purpose Business Continuity Management (including Crisis Management) competence and capability. It has five key functions:

1. To independently verify and validate compliance with the organisation's Business Continuity Management and Crisis Management policy, strategies, framework and good practice guidelines and/or standards adopted by the organisation
2. To independently review the organisation's Business Continuity Management solutions.

3. To independently verify and validate the organisation's Business Continuity Management and Crisis Management Plans.
4. To independently verify and validate that key exercising and maintenance activities are taking place, in line with the relevant programmes, processes and the organisations Business Continuity Management and Crisis Management framework and the good practice guidelines and/or standards adopted by the organisation.
5. To highlight key material 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 Business Continuity Management Practitioner. The Audit universe should be material to the organisation, clearly defined, documented and agreed in partnership with the relevant auditee and their senior management. Where an Auditor does not have the requisite professional level of Business Continuity Management knowledge, expertise and experience he should use a professional Business Continuity Management practitioner to assist in the audit.

Exercising.



Introduction.

The development a Business Continuity Management competence and capability is achieved through a structured and consistently applied exercising programme. To be successful an exercising programme must begin simply and escalate gradually. It is also important that only the resources that are planned to be available during and actual business continuity event and/or crisis are available during the exercise. The adoption and application of a structured and systematic approach to the development and implementation of an exercising programme will promote a greater understanding of the functioning of the Business Continuity Management process by all individuals associated with it.

In essence, exercising it is a generic phrase used to describe the critical Business Continuity Management process of exercising Business Continuity Management Strategies and Business Continuity Plans, rehearsing team members and staff and testing of systems (technology, telephony, administrative) to demonstrate a Business Continuity Management competence and capability.

Exercise:

- An act of employing or putting into use.
- Training.

Rehearsal:

- A 'practice' or 'drill'.

Test:

- A means of examination, a trial or proof.
- A 'pass' or 'fail' situation. Failure in the testing context must not be seen as a negative result. It is designed to ensure learning and continuous improvement. As a result 'failure' is considered a positive and beneficial outcome.

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 Business Continuity Management exercising makes the process more

acceptable and enables strengths to be acknowledged and weaknesses to be seen as opportunities for improvement rather than criticism.

The foundation of a successful exercising programme is dependent upon the positive professional commitment and active participation of staff, managers, directors and executives of the organisation who are confident and knowledgeable of their Business Continuity Strategy(ies) and Plan. Understanding and applying the 'Good Practice' guidelines is key to creating effective exercise scenarios. Good quality exercises will clearly identify areas for improvement. Consequently, the exercising process ensures that organisational Business Continuity Management remains current and viable in line with organisational change and current risk practice and appetite.

Purpose.

The purpose of exercising is twofold. The first is to evaluate and enable the continuous improvement of the organisation's Business Continuity Management competence and capability to achieve the prioritised recovery of its Mission Critical Activities and their dependencies within the Recovery Time Objective(s) and Recovery Point Objective(s) to ensure an approved minimum Level of Business Continuity (LBC). The second is to evaluate and enable the continuous improvement of the organisation's Crisis Management competence and capability.

Outcomes.

The outcomes of the Business Continuity Management exercising process includes:

- The identification of the organisation's Business Continuity Management maturity level.
- Verification and validation that the Business Continuity and Crisis Management Plan(s) and strategies are workable (feasible), effective, up-to-date and fit-for-purpose.
- Verification and validation that the organisation's crisis management competence and capability is effective, up-to-date and fit-for-purpose and will enable the management, control and co-ordination of a Business Continuity Management event at a strategic, tactical and operational level.
- Verification and validation that the team members and staff are familiar with and understand their roles, accountability, responsibilities and authority in the operation of the Business Continuity and Crisis Management process.
- The training/awareness of individuals involved in using the Business Continuity and Crisis Management Plan(s).
- The rehearsal and familiarisation of team members and staff with their roles, accountability, responsibilities and authority in the operation of the Business Continuity and Crisis Management Plan(s).

- Testing of the technical, logistical, administration and other operational systems of the Business Continuity and Crisis Management Plan(s).
- To test the Business Continuity Management organisation and infrastructure that includes command centres, work area, technology and telecommunications resource recovery.
- The rehearsal of the availability and relocation of staff.
- Verification and validation that the Business Continuity Plan reflects current business priorities.
- Verification and validation that the Business Continuity Plan incorporates all organisational Mission Critical Activities and their dependencies.
- The provision of a mechanism to reinforce Business Continuity and Crisis Management maintenance and auditing.
- A demonstrable Business Continuity and Crisis Management competence and capability.
- Documentation of exercise results for major customers, auditors, insurers, regulators and others.
- An increased awareness of emergency procedures.
- An increased awareness of the significance of Business Continuity Management.
- The opportunity to identify shortcomings and improvements to the organisation's Business Continuity and Crisis Management competence and capability e.g. strategy(ies), planning and Business Continuity Plan(s).
- The documentation and evaluation of the exercise to provide the foundation of a 'signed-off' and time driven 'action point' work schedule to improve the organisation's overall Business Continuity Management and Crisis Management competence and capability.

Components.

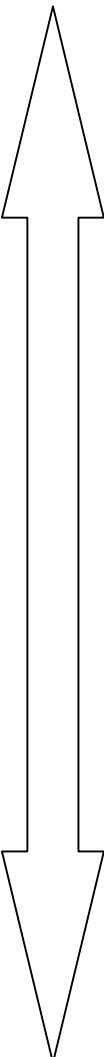
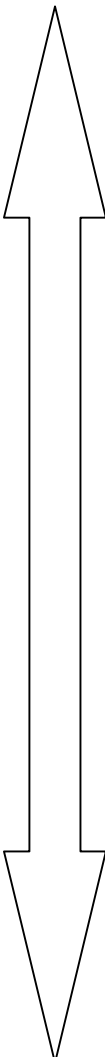
The key components of a Business Continuity Management exercise, rehearsal and/or test programme include:

- A clearly defined and documented Business Continuity and Crisis Management Exercising Programme, policy, strategy, framework and process that is approved and 'signed-off' by the executive/senior management of the organisation that includes:

- Scope e.g. solutions, strategies, plans, people and sourcing suppliers (both intra-organisation and outsourced providers).
 - Objectives i.e. outputs and deliverables.
 - Frequency and triggers.
 - Evaluation Criteria e.g. 'Good Practice' guidelines and standards; regulations and statute; effectiveness, up-to-date and fit-for-purpose.
 - Roles, accountabilities and responsibilities e.g. who is monitoring the implementation of the programme and who is undertaking the exercising activities.
 - Approach and Activities.
 - Process.
- A clearly defined and documented exercise contract (including objectives, scope, resources, schedules, success criteria) agreed and 'signed-off' by the manager of the organisation entity to be exercised and other key suppliers of logistic/services e.g. telecommunications, to enable the exercise to take place.
 - Business Continuity Management solutions e.g. work area recovery, staff relocation, Information Technology Disaster Recovery (ITDR).
 - Crisis Management.
 - Command and Control Centre(s)
 - Business Continuity Management/Crisis Management Teams.
 - Plan Do Check Act (PDCA) (BS779 version 2002)
 - Debriefing: Hot and Formal
 - Exercise Documentation:
 - Introduction package for participants.
 - Questionnaires
 - Learning 'Action Point' forms.
 - Scenario paper feeds.
 - Exercising Facilitator and Team.
 - Financial and other resources.
 - Exercise venue and facilities.
 - Exercise plan and timetable.
 - Post Exercise Report.
 - Post Exercise Action Plan.

Methodologies/Types/Techniques.

As identified earlier, exercising must be progressive and adopt a 'building block' approach. It is essential that an organisation should not overly ambitious in its initial exercising programme i.e. it should not attempt to run until it can walk. The traditional types, methods and techniques of exercising, their progression and potential combinations are illustrated in the following exercise matrix:

Type	Techniques	Process	Participants	Frequency	Complexity
Desk Check	<ul style="list-style-type: none"> Audit Validation Verification 	Review and Challenge the contents of the plan.	<ul style="list-style-type: none"> Author of plan Independent checker 	<p style="text-align: center;">High</p> 	<p style="text-align: center;">Low</p> 
Walkthrough Plan and/or Infrastructure	<ul style="list-style-type: none"> Scenario Freeplay 	Extended Desk Check to check interaction and the roles of participants	<ul style="list-style-type: none"> Author of plan Main participants 		
Simulation	<ul style="list-style-type: none"> Controlled Timelapse Unannounced Live Tabletop 	Incorporates associated plans: <ul style="list-style-type: none"> Business Site/Buildings Communication Public Relations ITDR BCM Resource Recovery Suppliers	<ul style="list-style-type: none"> Main Participants Facilitator Observers Co-ordinators Umpires 		
Functions	<ul style="list-style-type: none"> Individual Component(s) Integrated Components 	Moves to and recreates one or a number of business functions at an alternative pre-planned site.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> All employees and staff Facilitator Co-ordinators Umpires Observers BC Resource Recovery Providers 		
				Low	High

(Adapted from Source: Elliot, Swartz and Herbane 1999 p.84)

Process.

The key constructs of the exercising process include:

- Establish a meeting with the senior manager of the organisational entity to be exercised.
- Agree an exercise contract that is 'signed-off' by the senior manager of the organisation entity to be exercised and other key suppliers of logistics/services to enable the exercise e.g. telecommunications, to take place.
- Scenario Planning: prepare a representative, feasible, realistic and suitably detailed Business Continuity Management scenario (include aspects such as date, time, current workload, political and economic conditions, temporal/seasonal issues and critical timings e.g. end of financial year and current activities).
- Conduct a Risk Assessment of the exercise.
- Create an exercise:
 - management team (including support staff)
 - logistics/resource schedule
 - task checklist
 - infra-structure
- Scheduling Considerations: Careful consideration of the normal business cycle is needed to choose the best time to schedule and exercise to avoid disrupting the business at a crucial time.
- Exercise Documentation: Prepare questionnaires and learning/action point forms for distribution and use during the exercise to capture lessons learned by all players and observers involved in the exercise.
- Pre-exercise information and briefing of participants.
- Conduct exercise.
- Hot debrief.
- Formal debrief.
- Evaluate exercise and debriefing results and prepare a Post Exercise Report and recommendations.
- Post Exercise Report and recommendations agreed and 'signed-off' by the senior manager of the organisation entity that was exercised

- Create an agreed and 'signed-off' action plan to implement post exercise report recommendations i.e. update strategy and plan as approved, review exercising schedule for further exercising to prove the efficacy to the changes.
- Role accountable/responsible for Business Continuity Management within the organisation entity that was exercised 'signs-off' amended Business Continuity Management competence and capability (including strategies, plan and solutions) as effective, up-to-date and fit-for-purpose.

Frequency and Triggers.

The frequency of a Business Continuity Management Exercise Programme is dependent upon the nature, scale and complexity of the organisation and based on its business risk profile, appetite and the environment in which it operates.

- The Business Continuity Management Exercising Programme should include at least the minimum exercising requirement for the various Business Continuity Management components and the overall capability.
- The Business Continuity Management Exercising Programme should be circulated for consideration, consultation, comment and the approval of all participants prior to publishing the programme and before the development of individual exercise contracts.
- Business Continuity Management 'Good Practice' identifies that an exercise of the organisation's overall Business Continuity Management capability should take place at least once every 12 months (6 months for the three types of plan) unless:
- It is the initial development and documentation of the Business Continuity Strategy/Plan.
- Where the pace of business change is particularly aggressive a more frequent exercising programme may be necessary.
- The initial outsourcing and/or intra-organisation sourcing of a Mission Critical Activity or dependency.
- A significant change in the key technology and/or telecommunications including systems and/or networks.
- There is a major business change that may include:
 - Business strategy or objective.
 - Business Continuity Management strategy and/or scope.
 - Business Continuity Management solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation sourcing and/or outsourced providers)

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Post Business Continuity Management event.
- Process re-design.
- New business line or product or service.
- Merger.
- Acquisition.
- Significant change in the regulatory environment.

Participants.

The following roles or functions (not restrictive or exhaustive) are identified as being either Responsible, Accountable or should be either Consulted or Informed (RACI) in the exercise programme and its implementation. The matrix process provides a process that can be used to indicate/identify the specific roles, functions and/or area of the organisation within each of the RACI categories.

Role or Function	R	A	C	I
	Responsible	Accountable	Consulted	Informed
Executive/Senior Business Manager (Sponsor).				
Operational Middle Management.				
Operational Supervisors and Staff.				
Professional BCM Practitioner				
Exercise Facilitator				
Exercise Umpires				
Exercise Observers				
Exercise Support Team				
Exercise Players				
Health and Safety				
Risk Management (All types)				
Training and Development.				
Human Resources.				
Legal.				
Finance.				
Telecommunications.				
Technology.				
Facilities/Property Management.				
Suppliers of specialist Business Continuity Management resources and services (intra-organisation and/or outsourced providers).				
Insurance				

Emergency Services				
Security				
Local Authority Emergency Planning Officer				
Communications and Public Relations.				
Commercial Services Management.				
Relationship Management.				
Subject Experts (where appropriate).				
Suppliers of business services/products (intra-organisation and/or outsourced providers).				

Deliverables.

The deliverables of an organisation's Business Continuity Management Exercising Programme includes:

- A completed Business Continuity and Crisis Management Exercising Programme that is 'signed-off' by the organisation's executive/senior management.
- A clearly defined and documented Business Continuity Management Exercising Programme, policy, strategy, framework and process that is approved and 'signed-off' by the organisation's executive/senior management.
- A clearly defined and documented Post Exercise Report (including recommendations) approved and 'signed-off' by the senior manager of the organisation entity exercised.
- A clearly defined and documented Post Exercise Report Action Plan approved and 'signed-off' by the senior manager of the organisational entity exercised.
- An amended Business Continuity Plan that is 'signed-off' by the senior manager of the organisation entity that was exercised and/or plan owner (certify via document version control) as effective, up-to-date and fit-for-purpose.
- An amended Business Continuity Management Strategy(ies) that is 'signed-off' by senior manager of the organisation entity that was exercised and/or plan owner (certify via document version control) and/or organisation/s executive/senior management as effective, up-to-date and fit-for-purpose.

Good Practice Evaluation Criteria.

The 'Good Practice' Business Continuity Management Exercising evaluation criteria includes:

- Does the organisation have a clearly defined and documented Business Continuity Management Exercising Programme, policy, strategy, framework and process that is approved and 'signed-off' by the organisation's executive/senior management?
- Does the organisation's Business Continuity Management Exercising Programme provide a scheduled exercising cycle that is clearly documented with the organisation's Business Continuity Management Strategy(ies) and each Business Continuity Plan?
- Does the organisation have a clearly defined and documented standardised exercise contract that must be approved and signed-off' by the exercise sponsor and other participants prior to each scheduled exercise?
- Does the organisation's Business Continuity Management exercising, rehearsal and testing programme provide for various methods, types and techniques of exercising, rehearsal and testing e.g. desktop check, simulation?
- Has the organisation successfully demonstrated the Business Continuity Management of its Mission Critical Activities and their dependencies via exercising, rehearsal, testing or invocation?
- Does the organisation's exercising, rehearsal and testing programme evaluate the competence of both the team as a whole and its individual members?
- Does the organisations exercising, rehearsal and testing programme evaluate the overall Business Continuity Management capability of the organisation?
- Does the frequency of Business Continuity Management exercising, rehearsal and testing of the Business Continuity Management competence and capability reflect the organisation's environment, risk and potential business impact?
- Does the organisation use professionally qualified Business Continuity Management individuals to plan and facilitate Business Continuity Management exercises, rehearsals and tests?
- Does the organisation provide clearly defined and documented Business Continuity Management Exercising, Rehearsal and Testing Guidelines?
- Is a 'hot' debrief of all exercise, rehearsal or test participants carried out at the end of each BCM exercise, rehearsal or test?
- Does a organisation have a clearly defined and documented process that enables all participants of a BCM exercise, rehearsal or test encouraged to submit written

evaluations of the exercise, rehearsal or test process, results, any outstanding issues or lessons learnt?

- Does an exercise, rehearsal and/or test of the BCP occur after there is a major change in the organisation or its operating environment?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its BCM strategy?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its BCP?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its BCM capability?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of the relocation of its staff?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of the absence of its key staff?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its interim and manual processing procedures?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its work area recovery?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of the recovery and restoration of data (all mediums)?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its work backlog recovery?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its ITDR (technology) systems?

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its software?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its telecommunications?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its BCM team(s) competence?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its BCM command and control facility?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its command and control capability?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its Crisis Management capability?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its ability to function in the absence of key decision makers and management hierarchies?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its media a public relations capability?
- Has the organisation successfully demonstrated the BCM of its Mission Critical Activities and their dependency(ies) via exercising, rehearsal and testing or invocation in respect of its internal and external communications capability?
- Does the BCM testing of technical and telephony systems reflect their degree of complexity and coupling?
- Does BCM exercising demonstrate that business can access live systems and validate data and applications within the RTO and RPO identified by the BIA?
- Does the organisation have a clearly defined process to provide verification and validation that the Business Continuity Plan is being exercised in line with the organisation's Business Continuity Management Exercising Programme?

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Does the organisation have a clearly defined process to provide verification and validation that the Business Continuity Management teams are being rehearsed in line with the organisation's Business Continuity Management Exercising Programme.
- Does the organisation have a clearly defined process to provide verification and validation that the Business Continuity Strategy(ies) and resource recovery solutions are being tested in line with the organisation's Business Continuity Management Exercising Programme?
- Does the organisation use the Business Continuity Institute Good Practice Guidelines as a part of its Business Continuity Management Exercising Programme assurance process?
- Does the organisation have a clearly defined and documented process to provide a standardised format and content post exercise, rehearsal and/or testing evaluation report that is agreed and 'signed-off' by the BCP owner?
- Is there a clearly defined and documented post exercise process to provide an approved and 'signed-off' prioritised, time-scaled action plan to implement lessons learned, changes, improvements and amendments to the Business Continuity Plan, strategies and solutions as identified within the recommendations of the post exercise report?
- Does the Business Continuity Management documentation version control process i.e. 'signed-off' by the Business Continuity Plan owner, validate that the Business Continuity Plan has been amended to include the agreed recommendations from the post exercise report?

Further Reading.

Business Continuity Institute. (1999) ' Benchmarking Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (2000) ' The ten competencies of Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (1999) 'Getting Started: Business Continuity Management', Business Continuity Institute, Worcester.

Central Computer and Telecommunications Agency. (1995) 'An introduction to Business Continuity Management', HMSO, London. ISBN 0-11-330669-5.

Draper, B. (1998) 'Developing the IT plan', Continuity, Vol.2, No.3, pp.5-7.

Doughty, K. (2002) 'Business Continuity : A Business Survival Strategy', Information Systems and Control Journal, Vol.1. p.33.

Elliott, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management: Preparing for the worst', Income Data Services, London. ISBN 0-905525-56-6.

Federal Emergency Management Agency, (1998) 'Emergency Management Guide for Business & Industry' pp. 23-25 and 67.

Federal Reserve Bank. (2002) 'Summary of lessons learned and implications for business continuity', Federal Reserve Bank, New York, pp.1-10.

Ferguson, R.W. (2002) 'A supervisory perspective on disaster recovery and business continuity', Bank of International Settlement Review, pp.1-4.

Financial Services Authority. (2001) 'A risk focused review of outsourcing in the UK retails banking sector', Financial Services Authority, London, pp.1-19.

Financial Services Authority (2002) 'Working paper on Business Continuity Management', Financial Services Authority, London, pp.1-20.

Graham, G. (2000) 'Standard 8 - Maintaining and Exercising Business Continuity Plans', Continuity, Vol.4, Issue.2, p.14.

Grollmes, E.E. (1991) 'Disaster response plans minus drills equals unpreparedness', Disaster Management, Vol.3, No.3, p.122.

Halford, P. (2001) 'Addressing Business Continuity Management', Risk Management, Vol.6, No.1, pp.21-23.

Hemus, J. (1999) 'The simulation game', Continuity, Vol.3. Issue.3, pp.8-9.

Home Office (1996) ' Why exercise your disaster response', HMSO, London

Home Office (1999) 'The Exercise Planners Guide', HMSO, London.

Jackson, C. (2002) 'CSI Checklist: How the Sept 11 attack should impact your continuity planning', Computer Security Journal, Vol. XVIII, No.1, pp.1-7.

McLean, R. (2001) 'From incident to disaster: Managing the escalation process', Continuity, Vol.5, No.3, pp.6-9.

Mingay, S. (2001) 'Business continuity and the planning organisation: Tactical Guidelines', Gartner Group, London.

Newkirk, R.T. (2002) 'Facing the realities of the third millennium', The International Emergency Management Society (9th Annual Conference), pp.679-689.

Mitroff, I.I. and Pearson, C.M. (1993) 'Crisis Management: A diagnostic guide for improving your organisation's crisis preparedness', Jossey-Bass, San Francisco. ISBN 1-55542-563-1.

Moore, T. (1994) 'Planning and training for a major disaster', *Intersec*, Vol.4, Issue.10, pp.329-331.

Overy, B. (1993) 'The different types of exercise : When to use them', *Disaster Management*, Vol.5, No.4, pp.183-189.

Van-Haperen, K. (2001) 'The value of simulation exercises for emergency management in the United Kingdom' *Risk Management: An International Journal*, Vol.3, No.4, pp.35-50.

Video.

Business Continuity Institute (2001) 'Back to Business: Planning ahead for the unexpected', Merlin Communications Ltd, Cirencester, Gloucestershire.

Videotel International (1993) 'Crisis Management', Shandwick Communications, London.

Case Studies.

Automobile Association in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.79-87. ISBN 0-905525-56-6

Eurotunnel Fire in 1996 by Simpson, L. and Noulton, J.D. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.223-231. ISBN 0-33-72097-0

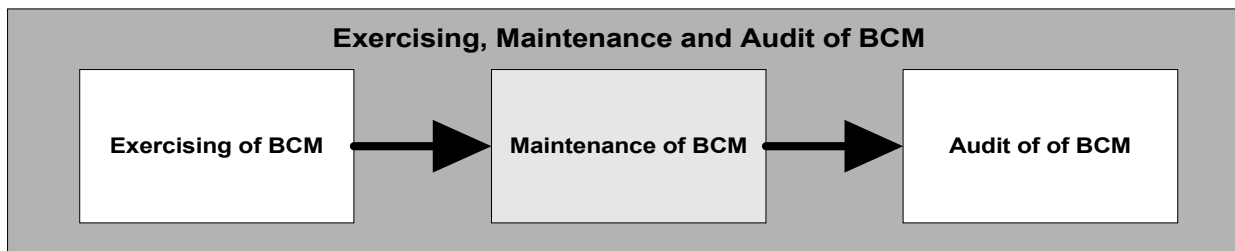
Federal Reserve Bank (2002) 'Summary of lessons learned and implications for business continuity', pp.1-10.

J. Sainsbury in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.113-122. ISBN 0-905525-56-6

Royal and Sunalliance (1996) 'Keeping a focus : The Manchester Effect - Do's and Don'ts'.

Worthington, J. (2002) 'Lessons for everyone from the Australian bush fires', *Continuity*, Vol.6, Issue.1, pp.7-9.

Maintenance



Introduction.

In contrast to many narrow plan based Business Continuity Management models the Business Continuity Management maintenance process is about maintaining the whole of an organisation's Business Continuity Management competence and capability and not just the Business Continuity Plan. This critical distinction is frequently overlooked by the organisations that consider Business Continuity Management to be a Business Continuity Plan.

The Business Continuity Management Maintenance Programme is concerned with a complex Business Continuity Management process and requires interaction with a wide range of managerial and operational roles from both a business and technical perspective.

Purpose.

The purpose of the Business Continuity and Crisis Management maintenance process is to ensure that the organisation's Business Continuity Management (including Crisis Management) competence and capability remains effective, fit-for purpose and able to achieve the recovery of its Mission Critical Activities and their dependencies within the Recovery Time Objective(s) to the Recovery Point Objective(s) and to ensure an approved minimum level of business continuity (LBC) of its services and products.

Outcomes.

The outcomes from the Business Continuity Management maintenance process include:

- Clearly defined and documented evidence of the proactive management and governance of the organisation's Business Continuity Management Monitoring and Maintenance Programme in respect of its Mission Critical Activities and their dependencies.
- Details of all changes to the Business Continuity Management strategy and Business Continuity Plans are clearly documented within the strategy history and version control details.
- Verification and validation that Business Continuity Management policy, strategies and plans continue to accurately reflect and be relevant to the organisation's business strategy, priorities, aims and objectives.
- The identification and inclusion of changes to the organisation's processes and systems.

- The identification and inclusion of changes to the industry's regulations and/or legislation.
- Verification and validation of the Business Impact Analysis and Risk Analysis upon which the Business Continuity Management Strategy(ies) and Business Continuity Plan(s) is based.
- Verification and validation that details within Business Continuity Management Strategies and Business Continuity Plans are up-to-date, accurate and complete.
- Verification and validation that the Business Continuity Management capability (including strategies and plans) are updated to reflect the lessons learned from exercising and/or their invocation.
- Verification and validation that Business Continuity Plans follow a logical sequence, format, structure, and conform to industry 'Good Practice' guidelines and standards
- Verify and validate that effective change (version) control process/ procedures are in place.
- Verify and validate that the organisation's Crisis Management competence and capability will enable the management/co-ordination of a Business Continuity Management event at an operational, tactical or strategic (corporate) level.
- Verify and validate that key people who will implement the Business Continuity Management strategy and plans remain in place, maintain a clear understanding of their roles and responsibilities and are familiar with the Business Continuity Management strategy(ies) and plans.
- Verify and validate that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Mission Critical Activities and/or their dependencies and/or business continuity recovery specialists remains effective and fit-for-purpose (as defined in contractual terms and conditions or service level agreements).
- The date of last and next Business Continuity Management maintenance review is clearly identified and documented together with the role named to complete the task.

Components.

The key components of a Business Continuity Management Maintenance Programme include:

- A clearly defined and documented Business Continuity Management Monitoring and Maintenance Programme policy, strategy, framework and process that should include:
 - Scope e.g. policy, framework, strategies, plans, people and suppliers.
 - Objectives i.e. outcomes and deliverables.
 - Frequency and triggers.
 - Evaluation Criteria e.g. 'Good Practice' guidelines and standards; regulations and statute; effectiveness, up-to-date and fit-for-purpose.
 - Roles, accountabilities and responsibilities e.g. who is monitoring the implementation of the programme and who is undertaking the maintenance activities.
 - Approach and Activities.

➤ Process.

- The organisation's Operational Business Strategy.
- Industry Business Continuity Management 'Good Practice' guidelines and standards e.g. ISO 17799 (IT Security).
- Contracts and Service Level Agreements of suppliers (intra-organisation and outsourced providers) of Mission Critical Activities and their dependencies.
- Contracts and Service Level Agreements of suppliers (intra-organisation and outsourced providers) of Business Continuity Management resources and services.
- The current 'signed-off' Business Impact Analysis of the organisation entity that is the subject of the maintenance programme.
- The current 'signed-off' Business Continuity Management strategies of the organisation entity that is the subject of the maintenance programme.
- The current 'signed-off' Business Continuity Plan of the organisation entity that is the subject of the maintenance programme.
- Legislative requirements.
- Regulatory requirements e.g. Financial Services Authority.
- The 'signed-off' Business Continuity Management exercise contracts, post exercise reports and action plans.
- The 'signed-off' Business Continuity Management audit report and action plans.
- The organisation's Business Continuity Management documentation that includes:
 - Policy.
 - Strategy(ies).
 - Framework.
- The current 'signed-off' Business Continuity Management Audit Report of the organisation entity that is the subject of the maintenance programme.
- The current 'signed-off' Business Continuity Management Exercise Report of the organisation entity that is the subject of the maintenance programme.
- The current 'signed-off' Business Continuity Management Assurance Report of the organisation entity that is the subject of the maintenance programme.

Methodologies/Techniques.

The methods, tools and techniques used to enable the Business Continuity Management maintenance process include:

- Robust Exercising Programme of plans and solutions
- Audit

- Assurance
- Benchmarking
- Current State Assessment 'Gap' Analysis
 - Questionnaires
 - Scorecards
 - Interviews (structured and unstructured)
- Risk Assessment
- Scenario Planning
- Training and awareness

Process.

The Business Continuity Management maintenance process includes:

- Clearly defining and documenting the Business Continuity Management Maintenance Programme e.g. for the whole organisation or its component parts based on a recognised frequency and triggers.
- Identify the key stakeholder roles and responsibilities i.e. those who are implementing and/or monitoring the implementation of the programme and those who are undertaking the maintenance activities.
- The Business Continuity Management Maintenance Programme is approved and 'signed-off' by the senior business manager and other key stakeholders.
- The Business Continuity Management Maintenance Programme should be embedded within the business as usual management processes of the part of the organisation e.g. department/site to which it specifically refers and it may be located within the Business Continuity Plan where appropriate.
- Review and challenge; verify and validate the various components of the Business Continuity Management competence and capability e.g. policy, strategies, solutions, plans, people and suppliers to ensure they are accurate, up-to-date and fit-for-purpose.
- This part of the process should be driven by the regular agreed frequency of the maintenance process for the various components of the Business Continuity Management capability or triggered by a clearly defined and documented event e.g. post exercise 'learning points' action plan, audit report and/or significant internal or external changes to the organisation or its environment.
- Business Continuity Management competence and capability updates, amendments and changes are identified, implemented and documented. These may include:
 - Strategy and policy issues signed off by the organisation's executive/senior management.
 - Strategy and plan issues 'signed-off' by the role accountable or responsible (where authorised) for the Business Continuity Management competence and capability of the organisation as a whole or a component part e.g. department/site.

- People and team issues 'signed-off' by the Business Continuity Manager.
- Supplier issues 'signed-off' by the executive/senior management or the organisation's relationship manager (where authorised) of the supplier.
- Assess whether changes and amendments create a training, awareness and/ or communication need.
- Scope training, awareness and/ or communication requirements.
- Delivery of appropriate training, awareness and/ or communication where applicable.
- Distribute updated, amended, changed Business Continuity Management policy, strategies, solutions, processes and plans to key stakeholders under the formal change (version) control process.

Frequency and Triggers.

The frequency of a Business Continuity Management Maintenance Programme is dependent upon the nature, scale and complexity of the organisation and based on its business risk profile, appetite and the environment in which it operates.

- The Business Continuity Management Maintenance Programme should include and clearly identify the minimum maintenance requirement for the various Business Continuity Management components and the overall capability.
- Business Continuity Management 'Good Practice' identifies that a maintenance review of the organisation's overall Business Continuity Management capability should take place at least one every 12 months (organisational level) and 6 monthly (business area/department level) unless:
- It is the initial development and documentation of the Business Continuity Management Strategy(ies)/Plan.
- Where the pace of business change is particularly aggressive a more frequent maintenance programme may be necessary.
- The initial outsourcing and/or intra-organisation sourcing of a Mission Critical Activity or dependency.
- A significant change in the key technology and/or telecommunications including systems and/or networks.
- There is a major business change that may include:
 - Business strategy or objectives.
 - Business Continuity Management strategy and/or scope.
 - Business Continuity Management solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation sourcing and/or outsourced providers)
 - Post Business Continuity Management event.
 - Process re-design.
 - New business line or product or service.

- Merger.
 - Acquisition.
 - Significant change in the regulatory environment.
- Business Continuity Management Strategy(ies)/Plans should be reviewed and updated, amended and/or changed as a part of the Business Continuity Management Maintenance Programme following exercises, rehearsals or tests where the post exercise report and action plan identifies and recommends improvements.
 - Business Continuity Management Strategy(ies)/Plans should be reviewed and updated, amended and/or changed as a part of the Business Continuity Management Maintenance Programme where a Business Continuity Management audit report and action plan identifies and recommends improvements.
 - Business Continuity Management Strategy(ies)/Plans should be reviewed and updated, amended and/or changed as a part of the Business Continuity Management Maintenance Programme where a Business Continuity Management assurance report and action plan identifies and recommends improvements.

Participants.

The following roles or functions (not restrictive or exhaustive) are identified as being either Responsible, Accountable or should be either Consulted or Informed (RACI) in the organisation’s Business Continuity Management Maintenance Programme and its implementation. The matrix process provides a process that can be used to indicate/identify the specific roles, functions and/or area of the organisation within each of the RACI categories.

Role or Function	R	A	C	I
	Responsible	Accountable	Consulted	Informed
Executive/Senior Business Management.				
Executive manager accountable for BCM within the organisation.				
Operational Middle Management.				
Operational Supervisors and Staff.				
Professional BCM Practitioner				
Owners of individuals BCP’s				
Members of the Crisis Management Team				
Members of the BCM Team				
Audit/Assurance				
Risk Management (All types)				
Training and Development.				
Human Resources.				
Legal.				
Finance.				
Telecommunications.				
Technology.				
Facilities/Property Management.				

Suppliers of specialist Business Continuity Management resources and services (intra-organisation and/or outsourced providers).				
Insurance				
Emergency Services				
Security				
Local Authority Emergency Planning Officer				
Communications and Public Relations.				
Commercial Services Management.				
Unions and staff associations				
Relationship Management.				
Subject Experts (where appropriate).				
Suppliers of business services/products (intra-organisation and/or outsourced providers).				

Deliverables.

The deliverables of an organisation's Business Continuity Management maintenance programme include:

- A clearly defined and documented Business Continuity Management monitoring and maintenance programme that is agreed and 'signed-off' by the executive/senior management accountable for an individual or several of the organisation's Mission Critical Activities and their dependencies.
- A clearly defined and documented Crisis Management monitoring and maintenance programme that is agreed and 'signed-off' by the organisation's executive/senior management.
- A clearly defined and documented Maintenance Report (including recommendations) agreed and 'signed-off' by the senior manager of the organisation entity to which the maintenance report refers.
- A clearly defined and documented Business Continuity Management Maintenance Report Action Plan agreed and 'signed-off' by the senior manager of the organisation entity to which the maintenance action plan refers.
- Effective, up-to-date and fit-for-purpose Crisis Management Plans, Business Continuity Plans, strategies and solutions concerning the organisation's Mission Critical Activities that are 'signed-off' by the plan/strategy/solution owner (certify via document version control) as being effective, up-to-date and fit-for-purpose.
- Clearly defined and documented due diligence reports that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Mission Critical Activities and/or their dependencies is effective, up-to-date and fit-for-purpose (as defined in contractual terms and conditions or service level agreements).

- Clearly defined and documented due diligence reports that the Business Continuity Management competence and capability of suppliers of Business Continuity Management recovery services (intra-organisation and/or outsourced providers) concerning the organisation's Mission Critical Activities is effective, up-to-date and fit-for-purpose (as defined in contractual terms and conditions or service level agreements).

Good Practice Evaluation Criteria.

The 'Good Practice' evaluation criteria for a Business Continuity Management Maintenance Programme includes:

- Does the organisation have a clearly defined and documented Business Continuity Management monitoring and maintenance policy, strategy, framework and process that includes:
 - Scope e.g. policy, framework, strategies, plans, people and suppliers.
 - Objectives i.e. outcomes and deliverables.
 - Frequency and triggers.
 - Evaluation Criteria e.g. 'Good Practice' guidelines and standards; regulations and statute; effectiveness, up-to-date and fit-for-purpose.
 - Roles, accountabilities and responsibilities e.g. who is monitoring the implementation of the programme and who is undertaking the maintenance activities.
 - Approach and Activities.
 - Process.
- Does the organisation's Business Continuity Management Maintenance Programme provide clear recognition that it is concerned with the whole of the organisation's Business Continuity Management capability and not solely Business Continuity Plan(s)?
- Are all changes to the organisation's Business Continuity Management documentation e.g. Strategy and BCP, clearly documented within the document history and version control details?
- Does all the organisation's Business Continuity Management documentation e.g. strategy and plans have clearly defined and documented change and version control procedure to ensure the integrity of the documents?
- Does the organisation's Business Continuity Management Maintenance process provide a clearly defined and documented maintenance process in respect of the whole organisations Business Continuity Management capability including the Business Continuity Plan?
- Does the organisation's Business Continuity Management maintenance process include the provision of clear and specific maintenance triggers to ensure all changes to Mission Critical Activities and their dependencies are formally brought to the attention of the role accountable and/or responsible for maintaining the Business Continuity Management competence and capability in respect of that Mission Critical Activity and/or its dependency(ies)?
- Does the organisation's Business Continuity Management maintenance programme provide a scheduled maintenance cycle that is clearly documented within the

organisation's Business Continuity Management Strategy(ies) and each Business Continuity Plan?

- Does the organisation's Business Continuity Management maintenance programme provide a clearly defined and documented challenge and review procedure and process e.g. planning and plan assumptions?
- Does the frequency of the Business Continuity Management maintenance programme reflect the nature, scale and complexity of the organisation and its environment, risk profile and appetite?
- Does the organisation use the Business Continuity Institute Good Practice Guidelines as a part of its Business Continuity Management Maintenance Programme assurance process?
- Does the organisation's Business Continuity Management maintenance process ensure that Business Continuity Management Plans, strategies and solutions concerning the organisation's Mission Critical Activities and their dependencies are 'signed-off' by the plan/strategy/solution owner as being effective, up-to-date and fit-for-purpose.
- Does the organisation have a clearly defined and documented Business Continuity Management maintenance (due diligence) process to ensure the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Mission Critical Activities and their dependencies is effective, up-to-date and fit-for-purpose (as defined in contractual terms and conditions or service level agreements)?
- Does the organisation have a clearly defined and documented Business Continuity Management maintenance (due diligence) process to ensure the Business Continuity Management competence and capability of suppliers of Business Continuity Management recovery services (intra-organisation and/or outsourced providers) concerning the organisation's Mission Critical Activities is effective, up-to-date and fit-for-purpose (as defined in contractual terms and conditions or service level agreements)?
- Is there a clearly defined and documented process to provide an agreed and 'signed-off' Business Continuity Management Maintenance Report and recommendations?
- Is there a clearly defined and documented process to provide a 'signed-off' time-scaled action plan to implement lessons learned, improvements and amendments to the organisation's Business Continuity Management capability as identified within either a Business Continuity Management exercise, audit or assurance report?
- Does the Business Continuity Plan documentation version control process i.e. 'signed-off' by the Business Continuity Plan owner, validate that the Business Continuity Plan has been amended to include the agreed recommendations from either a Business Continuity Management post exercise, audit and/or assurance report?
- Does the organisation's Business Continuity Management maintenance process provide a clearly defined and documented procedure to ensure that all changes to the Business Continuity Management strategy and/or Business Continuity Plan are agreed and 'signed-off' by the strategy/plan owner?
- Does the organisation's Business Continuity Management maintenance process provide a clearly defined and documented procedure to ensure that all changes to the

Business Continuity Management strategy and/or Business Continuity Plan are reflected in the Business Continuity Management exercising, training and awareness programmes?

- Does the organisation's Business Continuity Management maintenance process provide a clearly defined and documented procedure to ensure that all changes to the Business Continuity Management strategy and/or Business Continuity Plan are distributed to and received by all Business Continuity Plan holders?

Further Reading.

Business Continuity Institute. (1999) ' Benchmarking Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (2000) ' The ten competencies of Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (1999) 'Getting Started: Business Continuity Management', Business Continuity Institute, Worcester.

Central Computer and Telecommunications Agency. (1995) 'An introduction to Business Continuity Management', HMSO, London. ISBN 0-11-330669-5.

Graham, G. (2000) 'Standard 8 - Maintaining and Exercising Business Continuity Plans', Continuity, Vol.4, Issue.2, p.14.

Home Office. (1996) 'How resilient is your business to disaster?', HMSO, London.

Video.

Business Continuity Institute (2002) 'Back to Business: Planning ahead for the unexpected', Merlin Communications Ltd, Cirencester, Gloucestershire.

Videotel International (1993) 'Crisis Management', Shandwick Communications, London.

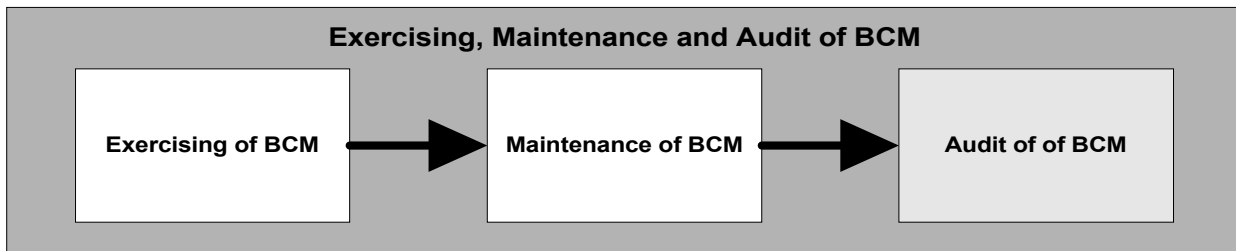
Case Studies.

Automobile Association in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.79-87. ISBN 0-905525-56-6

Honour, D. (2001) 'Heeding the lessons of 9/11', International Journal of Business Continuity Management, Vol.2, Issue.1, pp.13-17.

Royal Bank of Scotland in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.106-112. ISBN 0-905525-56-6

Audit.



Introduction.

A key focus and maxim in the auditing of an organisation's Business Continuity Management capability is the audit of the Business Continuity Management process and consequently the Business Continuity Management competence and capability. This approach recognises and assumes that if the process is correct and properly applied then the outcome should provide an effective and fit-for-purpose Business Continuity Management competence and capability.

The organisation's policy concerning the frequency and triggers concerning the auditing of Business Continuity and Crisis Management should be clearly defined and documented within the organisation's 'Audit Policy and Standards'.

The Business Continuity Management audit, like Business Continuity Management 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.

A key issue is the role and perspective of the auditor and audit function; it is one of impartial review against defined standards. Whilst the audit(or) may be fully aware and/or identify the reasons for Business Continuity Management shortcomings and organisational difficulties the audit has no option but to clearly identify the Business Continuity Management competence and capability gaps; this is an integral part of the objective of auditing as non-compliance is unacceptable. An integral part of the audit is also to provide remedial recommendations.

A further key consideration is that each stage of the Business Continuity Management life cycle requires may require a different audit approach. The audit approach is solely dependent upon the maturity of each stage of the Business Continuity Management life cycle i.e. none, novice, intermediate, advanced and mature.

Consequently the traditional proactive audit process should be seen as an enabling process to achieve a particular management objective(s).

Purpose.

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

Outcomes.

The outcomes from a Business Continuity Management audit include:

- Verification and validation that issues of operational resilience e.g. Mission Critical Activities and their dependencies have been identified and included in the organisation's Business Continuity Management strategies and plans.
- Verification and validation that the organisation's Business Continuity Management policy, strategies, framework and plans continue to accurately reflect and be relevant to the organisation's business strategy, priorities, aims and objectives.
- Verification and validation that the organisation's Business Continuity Management policy, strategies, framework and plans continue to accurately reflect industry 'Good Practice' guidelines and standards.
- Verification and validation that the organisation's Business Continuity Management competence is effective and 'fit-for-purpose'.
- Verification and validation that the organisation's Business Continuity Management capability is effective, up-to-date and 'fit-for-purpose'.
- Verification and validation that the organisation's Crisis Management competence and capability is effective, up-to-date and fit-for-purpose and will enable the management, command, control and co-ordination of a Business Continuity Management event at an operational, tactical and strategic (corporate) level.
- Verification and validation that the organisation's Business Continuity Management plan(s) are effective, up-to-date and 'fit-for-purpose'.
- Verification and validation that the organisation's Business Continuity Management solutions are effective, up-to-date and 'fit-for-purpose'.
- Verification and validation that the organisation's Business Continuity Management capability is compliant with relevant regulatory and legal requirements.
- Verification and validation that the organisation's Business Continuity Management Exercising Programme is being effectively implemented.
- Verification and validation that Business Continuity Management Strategies and Business Continuity Plans are updated to reflect the lessons learned from exercising and/or their invocation.
- Verification and validation that the organisation's Business Continuity Management Maintenance Programme is being effectively implemented.
- Verification and validation that Business Continuity Management Strategies and Business Continuity Plans are updated to reflect the lessons learned from the Business Continuity Management Maintenance Programme.
- Verification and validation that an effective documented change control process/procedure is in place and operating effectively.

- Verify and validate that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Mission Critical Activities and/or their dependencies remains effective and fit-for-purpose.
- Verify and validate that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Business Continuity Management specialist resources and/or services remains effective and fit-for-purpose.

Components

The key components of a Business Continuity Management Audit Programme include:

- A clearly defined and documented Business Continuity Management Audit Programme agreed and 'signed off' by the organisation's executive/senior management.
- A Business Continuity Management audit contract that is agreed and 'signed off' by the auditor and auditee. It is of critical importance that the framework and scope of an audit should be agreed and 'signed-off' by the senior management of the auditee(s) and not by the auditee(s) who is usually the operational manager of the business area to be audited.
- A Business Continuity Management audit plan for the organisation entity to be audited.
- Internal and external specialist/subject experts.
- Audit Standards
- Business Continuity Management (health check) scorecard.
- The Organisation's Business Strategy.
- The organisation's current Business Continuity Management strategy(ies).
- Contracts and Service Level Agreements of suppliers (intra-organisation or outsourced providers) of the organisation's Mission Critical Activities and their dependencies.
- Contracts and Service Level Agreements of suppliers (intra-organisation or outsourced providers) of Business Continuity Management specialist resources or services concerning the organisation's Mission Critical Activities and their dependencies.
- Regulatory requirements e.g. Financial Services Authority.
- Legislative requirements.
- Industry 'Good Practice' guidelines.
- Industry standards e.g. ISO 17799 (IT Security).
- Details of organisation's Business Continuity Management awareness and training programme.
- The 'signed-off' Business Continuity Management exercise contracts, post exercise reports and action plans.

- The current 'signed-off' Business Impact Analysis of the organisation entity being audited.
- The current 'signed-off' Risk Assessment of the organisation entity being audited.
- The current 'signed-off' assurance report of the organisation entity being audited.
- The previous 'signed-off' audit report (where appropriate) of the organisation entity being audited.
- The current 'signed-off' Business Continuity Plan of the organisation entity being audited.
- The organisation's documented Business Continuity Management Monitoring and Maintenance Programme.

Methodologies/Techniques.

The methods, tools and techniques to audit an organisation's Business Continuity Management programme include:

- Self (current state) assessment Business Continuity Management (health check) scorecard.
- Forensic (Investigative) Audit
- Compliance Audit
- Due Diligence Audit
- Feasibility Study Audit
- Project Management/Control Audit
- Best Value Audit

Process

The Business Continuity Management audit process includes:

- A Business Continuity Management audit contract and plan that is agreed and 'signed off' by the auditor and senior manager of the auditee (the auditee being the operational manager of the business area to be audited) and includes:
 - Clear identification and documentation of the type of audit to be carried out e.g. compliance, project management/control, feasibility study, due diligence or investigative.
 - Clear identification and documentation 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.

- Clear identification and documentation of the standard audit framework (where appropriate) to be used e.g. ISO/IEC 17799 (2000) IT security standards. The audit framework may be governed or restricted by legal or regulatory requirements.
 - Clear definition and documentation 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.
 - Determine the maturity level of the various stages of the Business Continuity Management life cycle in respect of the area/department/site to be audited.
 - The title of the audit should specifically identify that it is not solely based on information technology.
 - Clear definition and documentation 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
 - Granularity of audit.
 - Within the different levels at which Business Continuity Management is managed.
 - Within each stage of the Business Continuity Management life-cycle.
 - Within each entity of the organisation.
 - Clear identification and documentation of the audit evaluation criteria (standards).
 - Determine the requirement for specific subject expertise or third party assistance to conduct the audit.
 - Clear definition and documentation of the roles, accountability, responsibility and authority of key stakeholders i.e. those who will be conducting the audit and those who will be required to provide information and be interviewed.
 - Clear identification and documentation of financial and other audit resource requirements.
- Business Continuity Management Audit Programme requirements communicated to key stakeholders
 - Review and information gathering via the Business Continuity Management 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 a criteria for rating factual findings by using a clearly differentiated categorised predefined rating level (verbal or numerical).
- Double check that all planned audit steps have been completed, analysed and subjected to ratings.
- Provide a draft audit opinion report for discussion with key stakeholders.
- Provide an agreed and 'signed-off' audit opinion report incorporating recommendations as well as auditee responses where differences of opinion persist.
- Provide an agreed and 'signed-off' remedial action plan including timescales to implement the agreed recommendations of the audit report. This should also form a key element of the Business Continuity Management Maintenance Programme.
- Provide a monitoring process (in addition to the Business Continuity Management Maintenance Programme) to ensure that the audit action plan to address material deficiencies is implemented within the agreed timescale.

Frequency and Triggers.

The frequency of a Business Continuity Management Audit Programme is dependent upon the nature, scale and complexity of the organisation and based on its business risk profile, appetite and the environment in which it operates. The policy concerning the frequency and triggers of an audit should be clearly defined and documented within the organisations 'Audit Policy and Standards'.

- The Business Continuity and Crisis Management Audit Programme should include and clearly identify the minimum audit requirement for the various Business Continuity Management components and the overall capability.
- Good Business Continuity Management practice identifies that an audit of the organisation's overall Business Continuity Management capability should take place at least once every 12 months unless:
 - It is the initial development and documentation of the organisation's Business Continuity Management Strategy(ies) Plan.
 - Where the pace of business change is particularly aggressive a more frequent audit programme may be necessary.
 - The initial outsourcing and/or intra-organisation sourcing of a Mission Critical Activity or dependency.
 - A significant change in the key technology and/or telecommunications including systems and/or networks.
 - There is a major business change that may include:
 - Business strategy or objectives.

- Business Continuity Management strategy and/or scope.
- Business Continuity Management solutions.
- Location.
- Large scale change in staff numbers, locations or office densities.
- Key suppliers (intra-organisation sourcing and/or outsourced providers)
- Post Business Continuity Management event.
- Process re-design.
- New business line or product or service.
- Merger.
- Acquisition.
- Significant change in the regulatory environment.

Participants.

The following roles or functions (not restrictive or exhaustive) should be consulted and participate in the audit process. The matrix process provides a process that can be used to indicate/identify the specific roles, functions and/or area of the organisation within each of the RACI categories.

Role or Function	R	A	C	I
	Responsible	Accountable	Consulted	Informed
Auditor(s).				
Senior Management of auditee.				
Auditee.				
Operational Middle Management.				
Operational Supervisors and Staff.				
Professional BCM Practitioner.				
Risk Management.				
Members of the auditee's Crisis Management Team.				
Members of the auditee's BCM Team.				
Role accountable for auditee's BCM capability.				
Role responsible for maintenance of auditee's BCP.				
Training and Development.				
Human Resources.				
Legal.				
Finance.				
Telecommunications.				
Technology.				
Facilities/Property Management.				
Suppliers of specialist Business Continuity Management resources and services (intra-organisation and/or outsourced providers).				
Insurance				
Security				
Communications and Public Relations.				

Commercial Services Management.				
Relationship Management.				
Specialist or Subject Expert				
Suppliers of business services/products (intra-organisation and/or outsourced providers).				

Deliverables.

The deliverables of a Business Continuity Management Audit Programme includes:

- A clearly defined and documented Business Continuity Management audit contract agreed and ‘signed off’ by the senior management of the auditee.
- A clearly defined and documented Business Continuity Management audit plan (a statement of work and scope) agreed and ‘signed-off’ by the senior management of the auditee or organisation entity to be audited.
- An independent Business Continuity Management audit opinion report that is agreed and ‘signed-off’ by the senior management of the auditee.
- A clearly defined, prioritised and documented remedial action plan(s) that is agreed and ‘signed-off’ by the senior management of the auditee to implement the agreed recommendations of the independent Business Continuity Management audit report.
- A clearly defined and documented monitoring programme that is agreed and ‘signed-off’ by the senior management of the auditee to ensure that remedial action plans are implemented within the agreed timescale

Good Practice Evaluation Criteria

‘Good Practice’ Business Continuity Management Audit Programme evaluation criteria includes:

- Does the organisation have a clearly defined and documented Business Continuity Management Audit Programme that is set out in the Organisation (Corporate) Business Continuity Management Policy and Strategy?
- Does the organisation have an effective, robust and fit-for-purpose Business Continuity Management audit process?
- Does the scope of the Business Continuity Management audit programme focus on the organisation’s Mission Critical Activities their dependencies and single points of failure?
- Does the organisation’s Business Continuity Management Audit Programme provide a scheduled audit cycle that is clearly documented within the organisations Business Continuity Management Strategy(ies) and each Business Continuity Plan?

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Does the senior management of the auditee approve and 'sign-off' the Business Continuity Management audit contract and plan?
- Are the terms of reference and details of the Business Continuity Management audit clearly defined and documented in the audit contract?
- Does the Business Continuity Management audit contract clearly define and document the audit framework and process?
- Does the Business Continuity Management audit contract clearly identify appropriate standards, code of practice and other established audit models and frameworks?
- Does the Business Continuity Management audit framework take account (is it governed or restricted) by any legal, regulatory or statutory issues?
- Does the Business Continuity Management audit contract clearly identify the audit evaluation criteria/standards?
- Does the Business Continuity Management audit contract identify the business strategy objectives that are driving the audit?
- Does the Business Continuity Management audit framework take account (governed or restricted by) any regulatory, statutory or industry 'good practice' guidelines?
- Does the scope of the Business Continuity Management audit clearly identify and take account of the Business Continuity Management maturity stage of the whole or part of the organisation to be audited?
- Does the scope of the Business Continuity Management audit clearly define the type of audit to be conducted e.g. compliance, gap analysis, feasibility, due diligence or forensic?
- Does the scope of the Business Continuity Management audit provide clear objectives i.e. determine the questions that should be answered?
- Does the scope of the Business Continuity Management audit clearly indicate the area/department of the organisation to be audited i.e. it clearly indicates that the audit is not only on IT related matter?
- Does the scope of the Business Continuity Management audit contract clearly identify and prioritise the areas e.g. department, site to be audited?
- Does the Business Continuity Management audit contract clearly identify any external or other professional assistance needed to perform the audit?
- Does the Business Continuity Management audit contract clearly identify and document the level of detail/granularity for each audit item?
- Does the Business Continuity Management audit contract clearly identify the audit programme and timescales?
- Does the Business Continuity Management audit contract contain clear details of the audit financial and other resources?

- Does the organisation use the Business Continuity Institute 'Good Practice' Guidelines as a standard and an integral part of the Business Continuity Management Audit Programme?
- Does the organisation use the Business Continuity Institute 'Good Practice' Guidelines as a part of its Business Continuity Management Audit Programme assurance process?
- Is a prioritised and 'signed-off' (business and risk management) Business Continuity Management audit opinion report produced after each audit?
- Does the organisation have a process for escalating non-compliance issues as highlighted by individuals, dispensations, audit findings or crisis management process?
- Is a prioritised (business and risk management) 'signed-off' Business Continuity Management action plan to address issues identified during a Business Continuity Management audit prepared and implemented with a specific timescale?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management policy, strategies, framework and plans continue to accurately reflect and be relevant to the organisation's business strategy, priorities, aims and objectives?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management policy, strategies, framework and plans continue to accurately reflect industry 'Good Practice' guidelines and standards?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management competence is effective and 'fit-for-purpose'?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management capability is effective, up-to-date and 'fit-for-purpose'?
- Does the Business Continuity Management audit verify and validate that the organisation's Crisis Management competence and capability is effective, up-to-date and fit-for-purpose and will enable the management, command, control and co-ordination of a Business Continuity Management event at an operational, tactical and strategic (corporate) level?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management Plan(s) is/are effective, up-to-date and 'fit-for-purpose'?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management capability is compliant with relevant regulatory and legal requirements?
- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management Exercising Programme is being effectively implemented?
- Does the Business Continuity Management audit verify and validate that Business Continuity Management Strategies and Business Continuity Plans are updated to reflect the lessons learned from exercising and/or their invocation?

- Does the Business Continuity Management audit verify and validate that the organisation's Business Continuity Management Maintenance Programme is being effectively implemented?
- Does the Business Continuity Management audit verify and validate that Business Continuity Management Strategies and Business Continuity Plans are updated to reflect the lessons learned from the Business Continuity Management Maintenance Programme?
- Does the Business Continuity Management audit verify and validate that an effective documented change control process/procedure is in place and operating effectively?
- Does the Business Continuity Management audit verify and validate that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Mission Critical Activities and/or their dependencies remains effective and fit-for-purpose?
- Does the Business Continuity Management audit verify and validate that the Business Continuity Management competence and capability of suppliers (intra-organisation and/or outsourced providers) of Business Continuity Management specialist resources and/or services remains effective and fit-for-purpose?
- Does the Business Continuity Management audit policy provide for an independent Business Continuity Management audit reviews?
- Does the organisation's 'Audit Policy and Standards' clearly define the minimum standard frequency and triggers that the organisation's Business Continuity Management and Crisis Management capability must be audited?

Further Reading.

Business Continuity Institute. (1999) 'Benchmarking Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (2000) 'The ten competencies of Business Continuity Management', Business Continuity Institute, Worcester.

Business Continuity Institute. (1999) 'Getting Started: Business Continuity Management', Business Continuity Institute, Worcester.

Central Computer and Telecommunications Agency. (1995) 'An introduction to Business Continuity Management', HMSO, London. ISBN 0-11-330669-5.

Elliott, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management: Preparing for the worst', Income Data Services, London, ISBN 0-905525-56-6.

Fenn, D. (2002) 'Supplier Continuity: Managing risks across the supply chain', Continuity, Vol.6, No.1, pp.4-6.

Financial Services Authority. (2001) 'A risk focused review of outsourcing in the UK retail banking sector', Financial Services Authority, London, pp.1-19.

Financial Services Authority (2002) 'Working paper on Business Continuity Management', Financial Services Authority, London, pp.1-20.

Institute of Chartered Accountants in England and Wales. (1999) 'Internal Control: Guidance for directors on the Combined Code', Accountancy Books, London.

Mitroff, I.I. and Pearson, C.M. (1993) 'Crisis Management: A diagnostic guide for improving your organisation's crisis preparedness', Jossey-Bass, San Francisco. ISBN 1-55542-563-1.

Simms, J. (2001) 'Tick box management of business continuity plans', *Continuity*, Vol.5, Issue.2, pp.10-11.

von Roessing, R. (2002) 'Auditing Business Continuity Management', *Continuity*, Vol.6, No.3, pp.10-12.

Westmacott, P. (2001) 'Contingency Planning: Contractual Issues', *Continuity*, Vol.5, No.1, pp.6-7.

Video.

Business Continuity Institute (2002) 'Back to Business: Planning ahead for the unexpected', Merlin Communications Ltd, Cirencester, Gloucestershire.

Videotel International (1993) 'Crisis Management', Shandwick Communications, London.

Case Studies.

Automobile Association in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.79-87. ISBN 0-905525-56-6

British Telecommunications in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.88-96. ISBN 0-905525-56-6

Calor Gas in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.97-105. ISBN 0-905525-56-6

Thames Water in Elliot, D., Swartz, E. and Herbane, B. (1999) 'Business Continuity Management - Preparing for the worst', Income Data Services, London, pp.136-148. ISBN 0-905525-56-6