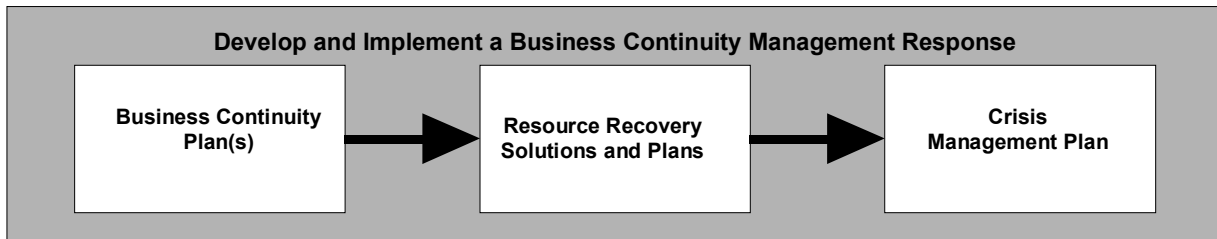


Stage 3 : Develop and Implement a Business Continuity Management Response.



Introduction.

Crises and Business Continuity Management (BCM) events have historically centred upon physical threats to geographic sites, buildings, people, mission critical activities and their dependencies regardless of size or location. However, as organisations, business and communication dynamics change so do the types of threats facing organisations. Whilst still exposed to physical threats an organisation is ever more exposed to reputation threats and attacks on its brand and image. Consequently, an organisation's reputation, image and brand, is judged by the media, markets, stakeholder and regulators upon its ability of effectively manage a crisis or business continuity event and continue to provide 'business as usual' services and products. The inability to fulfil these aims, or a badly positioned or wrongly perceived media response can result in a negative image and an increased negative media profile. These in turn may lead to regulatory, stakeholder or market pressures through concerns over the effectiveness of the organisation's Crisis and/or BCM competence and capability.

As far as is reasonably possible the different types of BCM and Crisis Management Plan(s) pre-define the actions that are necessary and the resources needed to achieve the objectives of the plan. The steps outlined in the plan are not intended to provide an exhaustive list or cover every eventually, as by their nature all events and crises are different. Consequently, the pre-defined procedures are not to be interpreted as the only course of action as it is recognised there may be an exceptional case where they may need to be modified to meet the needs of a specific (individual) business continuity or crisis event.

There are primarily three types of Business Continuity Management plan that may also be divided into a number of sub-plans e.g. communications:

- Business Continuity Plan.
- Business Continuity Resource Recovery and Solutions Plan.
- Crisis Management Plan.

The content and level of detail within each type of plan is dependent upon the nature, scale and complexity of the organisation and based upon its risk profile, appetite and the environment in which it operates.

A Business Continuity Management and Crisis Management Plan include a number of key constructs that include:

- Databases.
- Documents.
- Solutions
- Time based objectives.
- Tasks and activities required to achieve time-based objectives.
- Procedures/Processes.
- Information.
- Structure.
- Teams.

There are two main components to delivering an effective and fit-for-purpose Business Continuity Plan and Crisis Management Plan and their supporting capability:

- The formulation of the business continuity/crisis solutions, logistics and structure that support the plan;
- The development and documentation of the plan itself.

A further critical factor in the development of all of the different types of BCM plan is their exercising, rehearsal and testing (see Stage 5). In particular no plan should be considered complete until it has been exercised, rehearsed and tested and 'signed-off' as effective and fit-for-purpose by the plan owner and/or organisation's executive/senior management. This latter aspect further highlights the critical element of the competency of the human resources that enables the effective capability of the whole process

Business Continuity Plan: addresses business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed. They are based upon the agreed Business Continuity Strategies and provide procedures and processes for both the business continuity and resource recovery teams. In particular the plans allocate roles and their accountability, responsibility and authority. The plans must also detail the interfaces and the principles for dealing with a number of key issues e.g. internal/external communications, key suppliers, external bodies, emergency services and the media.

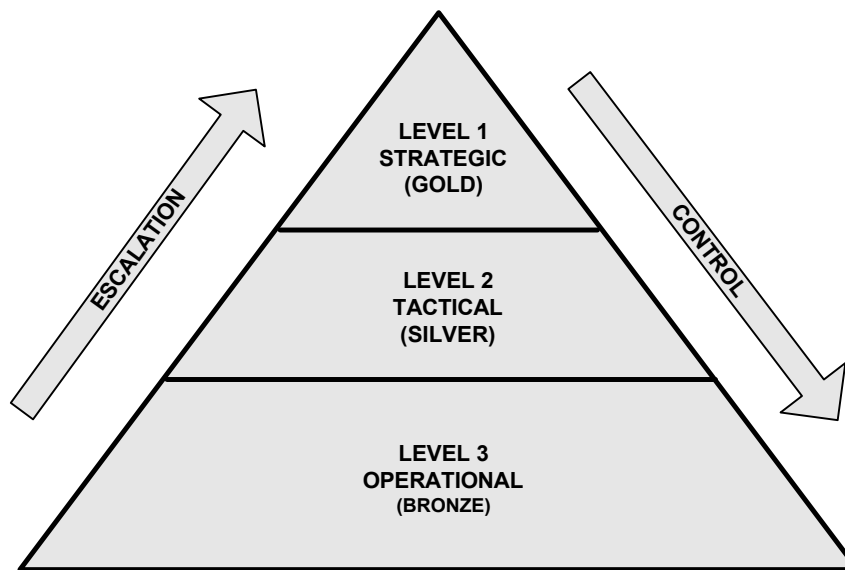
Business Continuity Recovery Solutions and Plan: concerns a number of BCM resources, solutions and approaches available to the BCM practitioner e.g. technical IT recovery (Server, WAN, LAN, etc), work area recovery, offsite storage.

Crisis Management Plan: is usually developed by large corporate organisations. It defines how the strategic issues of a crisis affecting the organisation would be addressed and managed. This component is vital in large and corporate organisations to ensure there is a robust and cohesive response to any crisis. This same crisis management response process and structure can be applied to any type of crisis and is not restricted to natural crisis situations e.g. earthquake, tornado, fire or flood but also man-made business and

industrial crises e.g. hostile take-over, credit risk, reputational risk, environmental pollution, criminal activity and health.

Crisis Management Structure and Escalation.

The crisis management structure should reflect the current organisational structure that will also provide the escalation process. This enables the most appropriate level of governance, ownership, control and response to be determined in respect of differing types of crises.



Level 1: is also known by the alternative names of Strategic or Gold. It is based on the executive or senior management command, control and co-ordination of the crisis where it is required at an organisational level. This level maintains a long term focus. The primary Level 1 functions include:

- Establish a framework of policy and strategy for the Level 2 team(s).
- Makes urgent executive decisions.
- Provide resources.
- Determine priorities
- Prioritise demands.
- Provide forward planning for returning to business as usual after the crisis has been resolved.
- Identifies and maximises opportunities or advantages arising from the crisis.

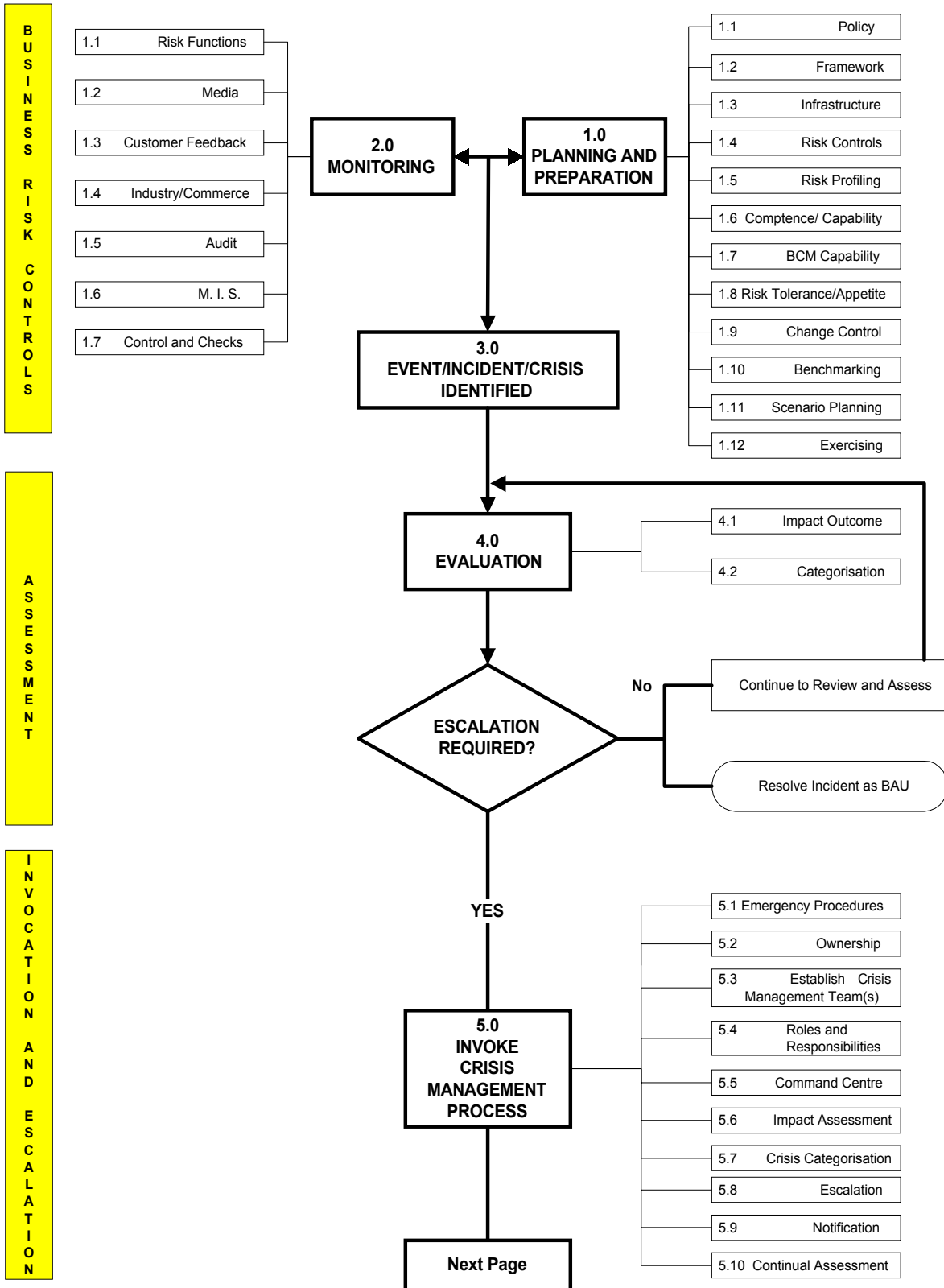
Level 2: is also known by the alternative names of Tactical or Silver. It is usually based on the 'hands-on' command, control and co-ordination of the crisis by the organisation's middle management. Consequently level 2 maintains a short term focus. The primary Level 2 functions include:

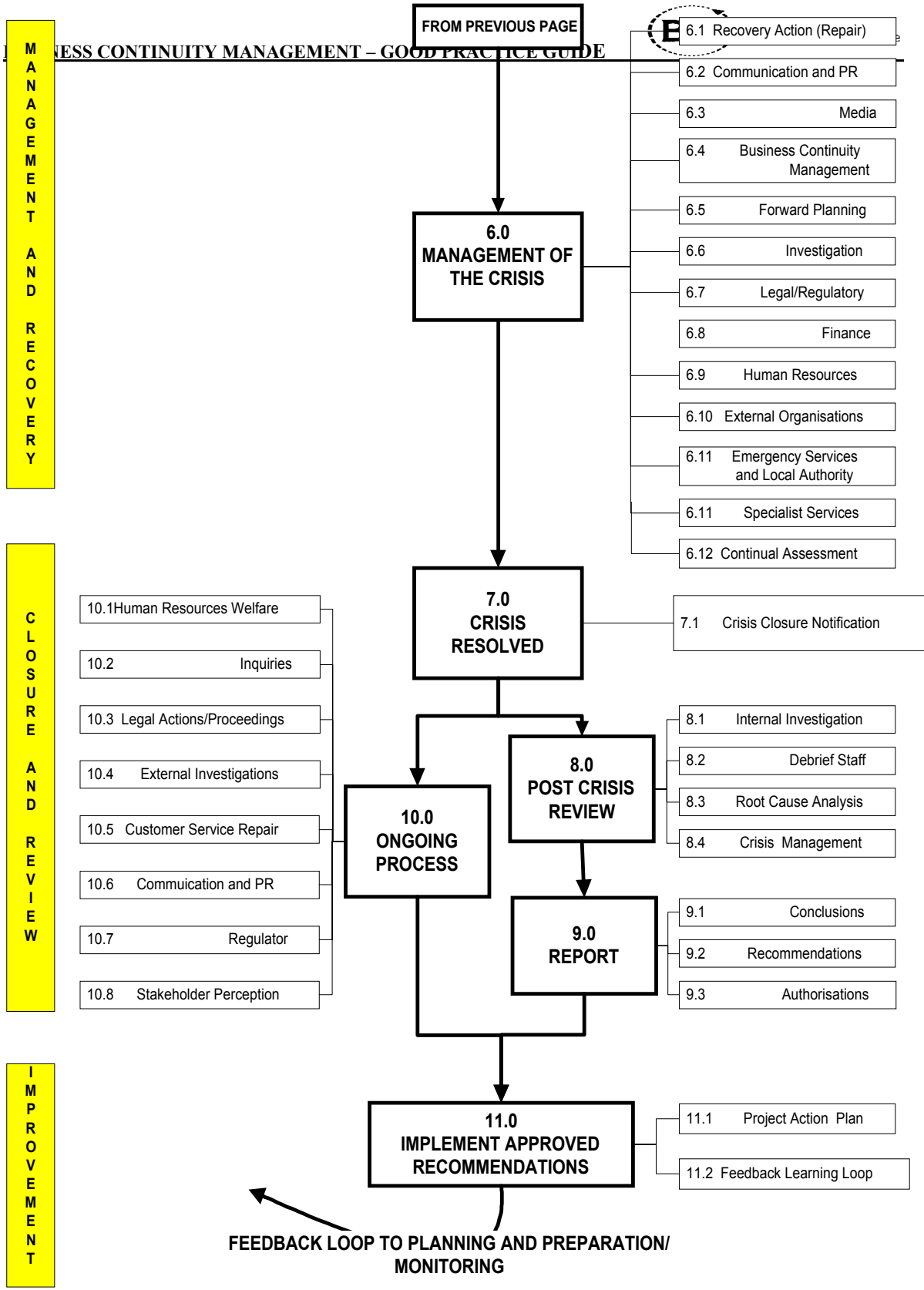
- Early emergency ‘damage limitation’ response.
- Determine the priority in allocating resources.
- Plan, co-ordinate and manage the implementation of the level 2 response.
- Obtain resources as required.

Level 3: is also known by the alternative names of Operational or Bronze. It is usually based on the organisation’s operational junior management, supervisors and staff. It deals with the ‘hands-on’ operational implementation of the crisis management strategy and consequently maintains a short term focus. Specifically the team(s) concentrate on their specific tasks within their area(s) of responsibility e.g. business area management, IT/technical management, facilities management, human resources management.

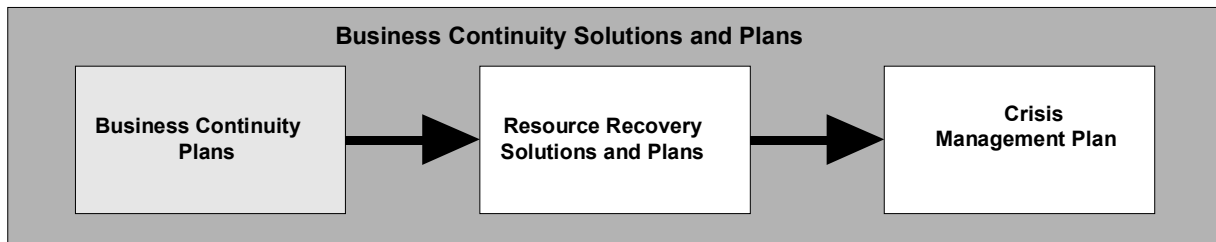
Crisis Management Process.

The following crisis management flowchart follows a natural escalation and identifies the high level activities and tasks that are necessary to deal with any event, incident or crisis. It illustrates a ‘total’ management process from the business controls that need to be implemented to prevent and prepare for a crisis to the learning and improvement process. The flowchart does not of itself provide the specific actions that need to be undertaken at the time of a crisis. These need to be detailed within the organisation’s crisis management plan.





Business Continuity Plans.



Introduction.

In contrast the general belief the development of a Business Continuity Plan does not signify the end of the BCM process but represents a milestone. A Business Continuity Plan does not provide a BCM competence or capability; it provides the approach to establishing an effective capability. Whilst the plan is of itself important it is a representation of the more important BCM planning process and a blue print to 'kick start' the response to a business continuity event. Consequently, it must be an 'action orientated' document.

The components and content of a Business Continuity Plan will vary from organisation to organisation and will have a different level of detail (granularity) based on criticality, importance and technical complexity. However, it should not include the following details that are not essential to the invocation and operation of the business continuity process:

- Business Impact Analysis.
- Risk Assessment.
- Exercise, Rehearsal or Testing Reports.
- Maintenance Process.
- Audit Report.
- Other non-essential information.

Purpose.

The purpose of a Business Continuity Plan(s) is to provide an effective, fit-for-purpose, predefined and documented framework and process to enable the Business Continuity Management of the organisation's Mission Critical Activities and their dependencies.

Outcomes.

The outcomes of the Business Continuity Plan include:

- A clearly defined and documented Business Continuity Plan to support the role of the organisation's BCM Team(s).
- Maximisation of the organisation's reputation and brand image.
- Maintenance of public, stakeholder, market and regulatory confidence and trust.

- Demonstrate effective and fit-for-purpose BCM and governance to the media, markets, customers, stakeholders and regulators.
- Limiting/preventing the impact of a BCM event.
- Minimising the impact of BCM event on the organisation's stakeholders by providing continuity of services, products and resources.
- The management of the business continuity or recovery of Mission Critical Activities and/or their dependencies within a timeframe (RTO) at an agreed service/production point (RPO) and minimum level business service/production continuity (LBC) that is established by a Business Impact Analysis and the organisation's risk appetite.
- The establishment of a clearly predefined and documented BCM response (solutions, timeline of activities and the recovery approach) following a business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed.
- Compliance with legal requirements.
- Compliance with regulatory requirements.
- A demonstration to stakeholders that the organisation has a BCM capability.
- A clearly defined and documented role owner of the Business Continuity Plan.
- Clearly defined BCM roles, accountability, responsibility and authority.

Components.

These guidelines set out the minimum standard of components and their content for a Business Continuity Plan (BCP). It is not intended to provide an exhaustive list to cover every eventuality, as by their nature all business continuity events are different. If the minimum standard is considered insufficient to meet the BCM needs of an organisation the additional requirements should be added to the Business Continuity Plan to enhance the minimum standard.

The structure (running order of the table of contents) of the Business Continuity Plan should also be customised to meet the specific needs of an organisation. Whilst a Business Continuity Plan structure is not mandated it is recommended that a standard Business Continuity Plan format be adopted to enable consistent application across an organisation.

Good practice identifies that a Business Continuity Plan should be modular in design with different consecutively numbered/named sections. The different sections provide an opportunity to form separate documents (modules) that can be supplied to individuals and/or teams on a need to know basis. There must be a clearly defined and documented control and change management process. The pagination of each section also provides for ease of reference. A further method is the production of the different modules and team plan on different coloured paper to provide ease of use and reference at the time of a BCM event.

The minimum standard components of a Business Continuity Plan include:

HEADER:

- Document classification (e.g. company confidential as per the organisation's classification policy).

FOOTER:

- Version control reference (including date).
- Page number.

FRONT PAGE:

- Title.
- Document classification e.g. company confidential as per the organisation's document classification policy.
- Version control i.e. version number, date, change author and change details.
- Management 'sign-off' of plan.
- Date of last plan review and role to carry it out.
- Date of next plan review and role to carry it out.

DISTRIBUTION LIST.

TABLE OF CONTENTS.

SECTION 1: PLAN OVERVIEW.

- Introduction.
- Purpose (Aim) of plan.
- Scope.
- Objectives.
- Assumptions.
- Plan ownership.
- Event/Decision Log.

SECTION 2: ACCOUNTABILITY, ROLES, RESPONSIBILITIES AND AUTHORITY

- **Site Business Continuity Management Co-ordinator:** The role of the Site BCM Co-ordinator occurs where large "campus" sites require co-ordination across different business areas. Each business area nominates its own Site BCM Co-ordinator. The role requires the nominated individual to use their business knowledge, experience and expertise to co-ordinate the business continuity efforts of their on-site business units in liaison with the individual business unit managers and the Site Crisis Management Team.
- **Business Unit Manager:** It is the accountability of the manager of each individual business unit to provide an effective 'fit for purpose' BCM capability for their specific business unit.
- **Business Unit BCM Team:** This team will be convened at the time of a BCM event (appointed in advance - with alternates) with the responsibility of implementing the business unit's BCM plan.

SECTION 3: NOTIFICATION, INVOCATION AND ESCALATION.

- Notification process and/or flowchart.
- Invocation process and/or flowchart.
- Escalation process and/or flowchart.
- Call out (call tree) cascade (including a reverse cascade) process and/or flowchart.

SECTION 4: BCM TEAM.

- BCM team membership.
- Location and contact details of BCM command centre(s).
- Map of BCM command centre location(s).
- Command centre resource profile.
- Battlebox.

SECTION 5: CONTACTS.

- External.
- Internal.
- Subject Experts.

SECTION 6: TASK CHECKLIST(S) AND AIDE MEMOIRES.

- Mandatory tasks.
- Discretionary tasks.
- Task completion tracking process.

SECTION 7: SUPPORTING INFORMATION.

- Personnel.
- Injuries and fatalities.
- Staff welfare and counselling.
- Media and public relations.
- Health and Safety.
- Emergency services liaison
- Finance.
- Legal advice.
- Suppliers (intra-organisation and outsourced providers).
- Insurance.
- Invocation of specialist services.
- Communications e.g. free-phone (0800) help lines.

SECTION 9: CRITICAL BUSINESS ACTIVITIES - RECOVERY ACTION PLAN.

- Schedule of Critical Business Activities or support activities.
- Critical Business Activities or support activities (RTO and RPO objectives) recovery action plan.

- Business Continuity Management resource recovery profile.
- Business Continuity Management recovery profile e.g. gantt chart.

SECTION 10: RECOVERY SITE LOCATION (Intra-organisation or outsourced supplier)

- Invocation process and/or flowchart.
- Recovery Site (work area) location floor plan layout.
- Map of Recovery Site location.
- Relocation of staff (including transport and accommodation).
- Security.
- Mail.

SECTION 11: RECOVERY RESOURCE PROFILE.

- Standard Workstations i.e. desk, chair, telephone and PC.
- Computer equipment.
- Software applications.
- Technology connectivity.
- Telecommunications.
- Telecommunications links.
- Backed-up data.
- Vital/unique documents/records.
- Office equipment.
- Specialist equipment.
- Stationary.
- Recovery Site location requirements e.g. disabled person access.

SECTION 12: FORM TEMPLATES.

- Meetings agenda.
- Internal briefings.
- Decision and action log.
- Task list status report.
- Telephone message.
- Action or task worksheet.

APPENDICES:

- Contracts and Service Level Agreements.
- Return Home.

Methodologies/Techniques.

The methods, tools and techniques to provide the planning and development of a Business Continuity Plan include:

- Current state assessment 'Gap' analysis.

- Questionnaire(s).
 - Scorecards.
 - Interviews (structured and unstructured).
-
- Stakeholder analysis.
 - Porter's Value Chain.
 - Scenario planning.
 - Checklists.
 - Workshops (facilitated by a professional BCM practitioner).
 - Generic minimum standard plan format and contents that can be customised. This approach enables standardisation in plan production and terminology. Another key benefit is that common escalation processes can be defined for the organisation.
 - A variety of business continuity planning and plan development software products are available but they are not essential to enable the successful development of a Business Continuity Plan. They can however provide significant benefits in the areas of plan maintenance and referential integrity.

Process.

The BCM professional has a key role in the planning and development of a BCM Resource and Solutions Plan. The professional BCM practitioners experience provides a valuable early 'reality' check in ensuring the BCM Resource and Solutions Plan(s) is/are appropriate, practical and workable.

The key constructs of the planning and Business Continuity Plan development process include:

- Appoint a role to be accountable/responsible for the BCM Resource and Solutions Plan.
- Define the scope of the plan.
- Define the objectives of the plan.
- Develop and approve a planning and plan development process and programme.
- Appoint a planning and plan development programme manager.
- Create a planning team (actual or virtual) to carry out the planning and develop the plan.
- Decide the structure, format, components and content of the plan.
- Determine the strategies on which the plan is based.
- Determine the key approaches to key phases of the plan.

- Conduct a BCM 'gap' analysis to establish the current state assessment.
- Gather information to populate the plan.
- Draft the plan.
- Circulate the draft of the plan for consultation, review and challenge.
- Gather feedback from consultation, review and challenge process.
- Amend plan as appropriate.
- Plan agreed and 'signed-off' pre-exercising by role accountable/responsible for the plan.
- Ongoing exercising, rehearsal, testing and maintenance of the plan to establish it is effective and fit-for purpose'.

Frequency and Triggers.

Whilst Business Continuity Plans should be reviewed on an ongoing basis the frequency and triggers that determine when a plan should be reviewed or audited 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 review or audit should be aligned with the review of other BCM related strategies, plans and solutions and be carried out at least every 6 months, unless:

- It is the initial development and documentation of the Business Continuity Plan.
- Where the pace of business change is particularly aggressive a more frequent review or audit 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.
 - BCM strategy and/or scope.
 - BCM solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation sourcing and/or outsourced providers)
 - Post BCM 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 or Accountable or should be either Consulted or Informed (RACI) in the planning and development of the Business Continuity Plan. 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
Site/Building/Business BCM Co-ordinator				
Operational Middle Management				
Operational Supervisors and Staff				
Risk Management				
Professional BCM practitioner				
Legal				
Finance				
Regulatory/Compliance/Audit				
Communications and Public Relations				
Telecommunications				
Technology				
Facilities/Property Management				
Human Resources.				
Suppliers of specialist BCM resources and services (intra-organisation and/or outsourced providers)				
Unions and Staff Associations				
Subject Experts (where appropriate)				
Suppliers of business services/products (intra-organisation and/or outsourced providers)				

Deliverables.

The deliverables of the Business Continuity Management planning process include:

- A clearly defined and documented Business Continuity Plan that is agreed and ‘signed-off’ by the accountable and/or responsible business owner of the Mission Critical Activity(ies) and/or their dependency(ies).

Good Practice Evaluation Criteria.

The Good Practice evaluation criteria of an organisation’s Business Continuity Plans include:

Business Continuity Management Planning.

- Does the organisation have a clearly defined, approved and 'signed-off' BCM planning process framework?
- Is the organisation's BCM planning process primarily concerned with the organisation's Mission Critical Activities, their dependencies and single points of failure?
- Does the organisation's BCM planning process clearly identify, address and comply with current regulatory requirements?
- Does the organisation's BCM planning process clearly identify, address and comply with current legal requirements?
- Does the organisation's BCM planning process clearly identify, address and comply with the organisation's current BCM Policy?
- Does the organisation's BCM process framework reflect the current BCI BCM Good Practice Guidelines?
- Does the organisation's BCM planning process clearly identify, address and comply with current legal requirements?
- Does the organisation's BCM planning process incorporate worst case 'Scenario Planning' e.g. loss of key staff, destruction of premises, systemic failure of technology and communications infrastructure?
- Does the organisation's BCM planning process consider various recovery scenarios via escalation procedures?
- Does the organisation's BCM planning process incorporate the use of stakeholder analysis?
- Does the organisation's BCM planning process clearly identify and address insurance issues?
- Does the organisation's BCM planning process clearly identify and mandate a clear desk policy?
- Is the planning process co-ordinated with the organisation's service/product sourcing (outsourcing and intra-organisation sourcing) providers?
- Is the organisation's BCM planning process integrated and co-ordinated with other parts of the organisation e.g. geographically/departments/sites?
- Do organisational managers fully understand their role in the BCM planning process?
- Are Business Continuity Plan (BCP) templates/frameworks/sample plans available for reference and to provide a standardised approach?

- Are professionally qualified BCM practitioners involved in the BCM planning process?
- Does the organisation have a clearly defined process to ensure that the learning points and/or recommendations arising from an exercising, rehearsal and testing programme and/or actual incidents (whether internally or externally) must be incorporated within the planning process?
- Does the organisation have a clearly defined process that must be employed to challenge and review the assumptions upon which the BCM strategy and plan is based?
- Are the Business Continuity Institute BCM Good Practice Guidelines used as a part of the Business Continuity planning/Plans assurance process?
- Does the Business Continuity Planning/Plans process achieve the Business Continuity Plans outcomes set out in the Business Continuity Institute BCM Good Practice Guidelines?
- Does the Business Continuity Planning/Plans process provide the Business Continuity Plans deliverables set out in the Business Continuity Institute BCM Good Practice Guidelines?

Business Continuity Plans.

- Does the Organisation have a clearly defined, up-to-date and fit-for-purpose Business Continuity Plan(s) for all its Mission Critical Activities, their dependencies and single points of failure?
- Does the BCP reflect the most up-to-date Business Impact Analysis (BIA) and Risk Analysis (RA)?
- Does the BCP clearly define the role of the accountable business owner of a plan?
- Has the BCP been approved and have a dated 'signed-off' declaration by its accountable business owner that it is up-to-date and fit-for-purpose?
- Does the BCP clearly identify and define the role that is accountable and/or responsible for its maintenance?
- Does the BCP clearly identify that it is an organisation confidential document?
- Does the BCP clearly identify that it should not be disclosed outside the organisation without written authority of the plan owner?
- Is the BCP of the organisation's Mission Critical Activities and their dependencies reviewed by the organisation's legal department/representative as a part of the planning process?
- Does the BCP establish a clearly predefined BCM response (solutions and recovery) following a business disruption, interruption or loss of the organisation's Mission Critical Activities and/or their dependencies from the initial response to the point at which normal business operations are resumed?

- Does the BCP clearly define the BCM and/or recovery of the organisation's Mission Critical Activities and their dependencies within as Recovery Time Objective (RTO) established by a Business Impact Analysis and the organisation's risk appetite?
- Does the BCP clearly define the BCM and/or recovery of the organisation's Mission Critical Activities and their dependencies to a Recovery Point Objective (RPO)?
- Does the BCP clearly define the BCM and/or recovery of the organisation's Mission Critical Activities and their dependencies to an agreed Level of Business Continuity (LBC -service/production/supply standard) within the Recovery Time Objective (RTO)?
- Does the BCP clearly define the BCM roles and their accountability, responsibility and authority?
- Does the BCP provide a clear and defined process for the independent review/audit of the plan at specific periods within the planning lifecycle?
- Do all BCP's within the organisation follow an integrated and agreed structure and minimum standard content?
- Does the BCP reflect the current BCI BCM Good Practice Guidelines?
- Does the BCP provide and define clear aims (purpose) and objectives?
- Does the BCP clearly identify and define the scope of the plan?
- Does the BCP contain a formal introduction?
- Does the BCP contain clear instructions on how to use the plan?
- Does the BCP contain clear details of how the plan is organised/structured?
- Does the BCP contain details of any assumptions either in its preparation or operation?
- Does the BCP contain a diagram of the BCM management structure?
- Does the BCP clearly distinguish between emergency response e.g. fire, and emergency BCM response, recovery and restoration?
- Does the BCP contain clear details and authority concerning purchasing and levels of financial spend?
- Does the BCP have a comprehensive Table of Contents?
- Does the BCP include a distribution list?
- Does the BCP contain a glossary of terms?
- Does the BCP contain a clear instruction that a copy of the plan is kept at both an on-site and off-site location?

- Does the BCP provide a clear timeframe schedule of the minimum resource requirements to achieve the RTO and RPO of each Mission Critical Activity and its dependencies?
- Is the distribution of the BCP strictly controlled e.g. numbered copies?
- Does the BCP clearly identify that it is an organisation confidential document?
- Does the BCP clearly identify that it shall not be used by other than authorised employees nor shall it be used or disclosed outside the organisation without authority?
- Does the BCP clearly identify and define a minimum exercising, rehearsal and testing programme to be completed within mandatory timescales?

Emergency BCM Response Procedures.

- Does the BCP provide a clearly defined, up-to-date and fit-for-purpose BCM emergency response and evacuation procedures and evacuation and assembly points for different types of incident e.g. fire/bomb?
- Does the BCP provide clear and detailed instructions on how to activate the BCM emergency response procedures in contrast to emergency procedures e.g. fire?
- Does the BCP provide a clearly defined process for the application of containment measures in respect of damage and the overall impact of the incident?
- Does the BCP provide a clearly defined process and criteria to define and classify any damage and the overall impact of the incident?
- Does the BCP provide a clearly defined process to ensure there are links to other organisations e.g. emergency services, suppliers that may be involved in the recovery and restoration process?

Notification, Invocation and Escalation.

- Does the BCP have a clearly defined and structured up-to-date and fit-for-purpose BCM notification, invocation and escalation process?
- Does the BCP contain clearly defined instructions as to whom has the authority to invoke (other than where it is self-evident) the BCP?
- Does the BCP contain a clearly defined notification, invocation and escalation process flowchart?
- Does the BCP contain a clearly defined call-out and information cascade process flowchart?
- Does the BCP contain clearly defined process for notifying the organisation's legal department/representatives?

- Does the BCP contain clearly defined process for notifying the organisation's media and public relations department/representatives?

Roles, Accountability, Responsibility and Authority.

- Is the role of organisation's executive/senior management during a BCM event clearly defined, agreed and documented?
- Has the overall accountability and/or responsibility for the management of the BCM process within the organisation clearly defined and documented?
- Has a senior manager (executive) been appointed as accountable for BCM within the organisation?
- Does the BCP contain clearly defined instructions, advice, guidance and process concerning the authorisation of financial expenditure during a BCM event?
- Have the various BCM teams been established for the business continuity of Mission Critical Activities and their dependencies?
- Does the BCP clearly set out and define BCM team roles and their responsibilities, accountabilities and authorities?
- Are all key staff fully aware of their BCM roles, accountabilities, responsibilities and authority?
- Does the BCP contain details of any reservations concerning role accountability, responsibility or authority in its operation?
- Does the BCP contain details of any exclusions concerning role accountability, responsibility or authority in its operation?
- Does the BCP contain clearly defined instructions, advice, guidance and process concerning the authorisation of financial expenditure?
- Has each BCP role been assigned to a principal individual?
- Has each BCP role been assigned to an alternate individual should the principal be incapacitated or otherwise unavailable?
- Has each BCP role been allocated to an appropriate level of authority to carry out the role accountabilities and/or responsibilities?
- Are all managers aware of their responsibilities to ensure compliance with the legal, regulatory and policy requirements for crisis management?
- Does the role and responsibility of each BCM team include the criteria for invoking all or its specific part of the BCP?

Key Supporting Information.

- Does the BCP contain either mandatory instructions, advice, process, procedure or guidelines concerning key supporting information?

People Issues.

- Does the BCP contain either mandatory instructions, advice, process, procedure or guidelines concerning casualties and fatalities?
- Does the BCP contain either mandatory instructions, advice, process, procedure, guidelines or service concerning confidential staff counselling?
- Does the BCP contain mandatory instructions, advice, process, procedure or guidelines concerning staff welfare e.g. personal belongings, travel and relocation issues?
- Does the BCP contain mandatory instructions, advice, process, procedure or guidelines concerning staff and public announcements?
- Does the BCP requirements and arrangements realistically reflect the needs of individual personnel and their commitments?
- Have the organisation's Human Resources Department been consulted in the development of the organisation's BCM strategy(ies)/plan(s)?
- Have Trade Unions and Staff Associations been consulted in the development of the organisation's BCM strategy(ies)?
- Are Trade Unions and Staff Associations consulted in the development of individual BCP's?

Communication.

- Does the BCP contain mandatory instructions, advice, process, procedure or guidelines concerning internal and external communications?
- Does the BCP have a clearly defined communication process (e.g. 0800 free phone) to ensure staff and all other stakeholders are kept informed?
- Does the BCP provide a clearly defined process for notifying staff and other stakeholders of new/different telephone/fax numbers?
- Does the BCP have a clearly defined and circulated business help-line to deal with customer and client enquiries?
- Does the BCP provide a clearly defined reverse cascade callout/communications process to enable the safety of staff to be confirmed?

- Does the BCP provide a clearly defined response to the failure of voice and/or data communication systems?
- Does the BCP have a clearly defined, up-to-date and auditable callout (call tree) cascade process?
- Does the BCP provide approved preformatted messages?
- Does the BCP clearly identify relevant stakeholder groups and establish essential communication plans with them?
- Does the BCP provide a clearly defined process for redirecting telephony and fax communications?
- Does the BCP provide a clearly defined process and information for notifying the BCM team(s) and maintaining lines of communication to its members?
- Are staff and managers provided with a pocket-size BCM aide memoire?

Documentation/Forms/Checklists.

- Does the BCP have an up-to-date task list that clearly identifies both mandatory and discretionary tasks together with the individuals accountable/responsible for their completion with an allocated timeframe?
- Does the BCP provide an auditable process for tracking and recording the completion of the BCP task list after the plan has been invoked and any additional/further on-going tasks?
- Does the BCP provide an auditable process for tracking and recording the completion of additional/further ongoing tasks in addition to those contained within the BCP tasks list?
- Does the BCP provide up-to-date (internal and external) contact schedules/lists (e.g. key and alternate staff, suppliers, stakeholders)?
- Does the BCP provide an incident management and decision log template?
- Does the BCP provide an impact assessment profile template?
- Does the BCP provide an up-to-date minimum resource BCM recovery profile?
- Does the BCP provide a telephone message form/log?
- Does the BCP provide a Recovery Status Report template?
- Does the BCP provide a Business Relocation Recovery Profile?
- Does the BCP provide a list of the contents of the battlebox?
- Does the BCP contain copies of relevant contracts, Service Level Agreements, memorandums of understanding and letters of agreement?

External Bodies and Organisations.

- Has an Emergency Services Liaison Officer been appointed?
- Have statutory/regulatory/official agencies been identified and included in the organisation's BCM planning process?
- Does the BCP provide clearly defined co-ordination procedures for local authorities?
- Does the BCP provide clearly defined co-ordination procedures for other relevant public authorities?
- Does the BCP provide clearly defined co-ordination procedures for service utilities?

Media and Public Relations.

- Does the BCP provide clearly defined process for dealing with the media and public relations during a BCM event?
- Does the BCP clearly identify and unambiguously describe stakeholders and interest groups?
- Does the BCP provide clearly defined and prepared generic media statements?
- Does the BCP clearly identify external liaison points e.g. organisations, agencies and individuals?
- Does the BCP clearly identify individuals who have been trained to deal with the media?

Further Reading.

- Birch, D. (2002) 'Business Continuity for telecommunications', *Continuity*, Vol.6, No.1, pp.10-13.
- Business Continuity Institute (1999) 'Benchmarking Business Continuity Management', BCI, Worcester.
- Business Continuity Institute (2000) 'The ten competencies of Business Continuity Management', BCI, Worcester.
- Business Continuity Institute (2001) 'Getting started', BCI, Worcester.
- Central Computer and Telecommunications Agency, (1995) 'An introduction to business continuity management', HMSO, London. ISBN 0-11-330669-5.
- Charters, I. (2000) 'The reality of worst case scenarios', *Continuity*, Vol.4, No.4, pp.7-8.

- Elliott, D., Swartz, E., and Herbane, B. (1999) 'Just waiting for the next big bang: Business Continuity in the UK financial sector', *Journal of Applied Management Studies*, Vol.8, No.1, pp.43-60.
- 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 Reserve Bank, (2002) 'Implications of 9/11 for the financial services sector', *Bank of International Settlement Review*, pp.1-5.
- Ferguson, R.W. (2002) 'A supervisory perspective on disaster recovery and business continuity', *Bank of International Settlement Review*, pp.1-4.
- 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', FSA, London, pp.1-19.
- Financial Services Authority. (2002) 'FSA working paper on Business Continuity Management', FSA, London, pp.1-20..
- Frost, C. (1994) 'Effective responses for proactive enterprises: Business continuity planning', *Disaster Prevention and Management*, Vol.3, No.1, pp.7-15.
- Home Office. (1996) 'How resilient is your business to disaster', HMSO, London.
- Honour, D. (2001) 'Heeding the lessons of 9/11', *International Journal of Business Continuity Management*, Vol.2, No.1, pp.13-17.
- Kirvan, P.F. (2000) 'Business continuity strategies for call centres', *Continuity*, Vol.4, No.2, pp.9-10.
- McLean, R. (2001) 'From incident to disaster: Managing the escalation process', *Continuity*, Vol.5, No.3, pp.6-9.
- Moore, P. (2001) 'Ensuring business continuity for vital business systems', *Risk Management*, Vol.6, No.1, pp.29-31.
- Porter, M.E. (1985) 'Competitive Advantage: Creating and sustaining superior performance', Free Press, New York.
- Power, P. (1999) 'Business Continuity Management: Preventing chaos in a disaster', Department of Trade and Industry, London.
- Simms, J. (2002) 'Tick box management of business continuity plans', *Continuity*, Vol.5, No.2, pp.10-11.
- Smith, D.J. (2001) 'A receipt for chaos', *Risk Management*, Vol.6, No.1, pp.9-14.

Videos.

British Telecommunications (1995) 'The Foresight Saga: Planning for Continuity of Communications', British Telecommunications Plc, London.

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

Royal and Sunalliance (1996) 'The Manchester Bombing Incident', Elite Television, Leeds.

British Council for Shopping Centres (1999) 'Shopping Centre Bomb Threats', Williams Management Communication, London.

Case Studies.

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.

Graham, J. (1999) 'Managing your way back from the brink', Continuity, Vol.3, Issue.1, pp.4-7.

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

Mellish, S. (2000) 'When a BCP really comes into its own', Continuity, Vol.4, Issue4, pp.4-6.

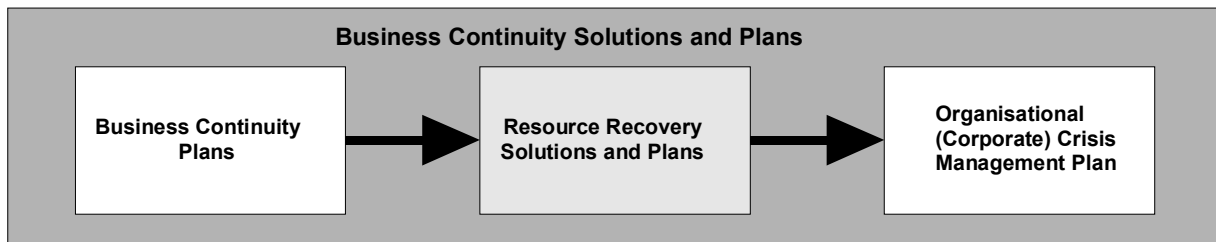
Manchester Bombing in 1996 in HMSO (1999) 'Business As Usual - Maximising business resilience to terrorist bombings', pp.6-10.

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

Stena Challenger Grounding in 1995 by Simms, J. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.181-192. ISBN 0-33-72097-0

The aftermath of multiple murder in 1995 by Street, J. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.208-213. ISBN 0-33-72097-0

Resource and Recovery Solutions.



Introduction.

It is not possible to provide an exhaustive list of potential operational resilience and business continuity resource recovery solutions as this will vary dependent upon the activities performed and the risk appetite of the organisation. However, resiliency measures and resource recovery solutions should be prioritised and tiered dependent upon their criticality to the organisation as defined by the Business Impact Analysis(BIA).

Where a Business Continuity Management solution is supported by a contractual commitment it is usually only for the lifetime of the contract. As a result it is critical that in addition to the option of renewing the contract that the terms and conditions enable the variation (resilience) of the agreed level of service provision i.e. the upsizing or downsizing together with the associated cost.

Purpose.

The purpose of a Business Continuity Management Resource Recovery Plan and solution planning is to provide the key components that support the organisation's Business Continuity Plan(s).

Outcomes.

The outcomes from a Business Continuity Management Resource Recovery Plan and solution planning includes:

- Effective, up-to-date and fit-for-purpose BCM resource recovery solutions for Mission Critical Activities their dependencies and single points of failure.
- Resilient and business continuity protected Mission Critical Activities their dependencies and single points of failure.
- Contracts and/or Service Level Agreements for specialist BCM services, products and/or resources with either intra-organisation sourcing or outsourced providers.
- Change control process to ensure that BCM resource recovery solutions for Mission Critical Activities their dependencies and single points of failure remain effective, up-to-date and fit-for-purpose.

Components.

The following are examples of the type of business continuity resource recovery solution options that should be considered:

- **Insurance:** Insurance is often seen as the first BCM option to be considered as a consequence of its impact on the financing of other options. Whilst it provides considerable benefits there are other considerations that recognise it does cover the loss of market share, shareholder value, reputation and brand tarnish.
- **Resilient Operations:** Options include active/active operations and continuous availability solutions. These options are normally amongst the more expensive to implement but provide good levels of protection for Mission Critical Activities. Large organisations would find this appropriate for high value, same day payment processing but the cost may be prohibitive for less critical operations. When considering resilient operations it is vital to identify and resolve all single points of failure.
- **Work Area Recovery:** The key issue is whether contingency office accommodation is provided in-house or externally by specialist third party suppliers. In most large organisations it is a mixture of both based on the organisation's BCM Resource Recovery Strategy and cost. Third-party suppliers provide a range of solutions covering dedicated, syndicated or mobile solutions. The most effective option is dependent upon criticality as well as recovery timescales with dedicated providing guaranteed availability but being the most expensive. The general recovery periods are:
 - Dedicated - immediate recovery
 - Syndicated - 4 hour plus recovery
 - Mobile - minimum of 4 days (build periods differ based on location and local conditions).

Syndication Ratios: The general industry trend is a maximum of 25 to 1 i.e. each desk is sold a maximum of 25 times, but great care should be taken to understand who are the other 24 customers potentially using each desk e.g. some suppliers provide client details by post code. The parameters acceptable to an organisation should be clearly defined within its BCM Resource Recovery Strategy and should not be left to individual contract negotiations.

Exclusion Zones: The organisation's definition of exclusion zones should be clearly defined within the corporate BCM Strategy e.g. within the City of London a 800 metre exclusion zone (vehicle size bomb) is the minimum acceptable standard.

- **Remote Working:** This option includes the concept of "working from home" and working from other non-corporate locations e.g. hotels. Working from home can be a very effective solution but care must be taken to ensure Health and Safety issues are addressed and sufficient dial-up capacity is available. Due to security and confidentiality issues this option is not always suitable.
- **Displacement:** This option is basically the displacement of non-critical operations and staff (at a suitable alternative location) by staff performing a higher priority (time critical) activity e.g. a Mission Critical Activity dependency. This option is often most valuable as a temporary low-cost solution whilst mobile recovery solutions are developed. Care

must be taken when using this option that a backlog of non-critical work suddenly becomes critical.

- **Data Centre(s):** Data Centre recovery strategy and solutions must be agreed at a corporate level. There are a number of options that can provide a suitable solution including in-house recovery or third party (bureau) support. It is vital that both Recovery Time Objectives and Recovery Point Objectives are agreed and tested.
- **Telephony:** The redirection of telephony to alternative locations can be a problematic. It is important that resilience and flexible solutions are implemented to support 'Business As Usual' and where necessary critical customer service numbers are converted to '0845' or similar numbers that allow quick and simple redirection.
- **Call Centre(s):** The issue is a convergence of IT and telephony which may provide significant recovery challenges. Again it is important that resilience is in-built into 'Business As Usual' processing to allow redirection of telephony and supporting **IVR** processing. The Active/Active approach is the preferred design for call centre operations with most organisations having a number of call centres which load share.
- **Electronic Commerce:** Electronic Commerce now provides core business services that must be covered by BCM. The Internet can also provide an excellent vehicle for communications and broadcasts via the corporate Internet website and Intranet.
- **Technical/Server Resilience and Recovery:** On-site Information Technology (IT) resilience and recovery is a key issue with more and more Information Technology capacity being devolved into the business areas. There are a number of solutions available and the most appropriate will be based on Recovery Time Objectives and Recovery Point Objectives. Specialist Information Technology support may be required in defining and developing the technical resilience and recovery solutions.
- **Ship in Contracts:** This type of solution is very cost effective where a recovery capability can be built up following an incident or disaster. It normally covers mobile buildings, IT equipment such as PCs, servers and printers but can also cover specialist equipment.
- **Paper/Critical Documents/Vital Records:** Solutions include off-site battle boxes, fireproof cabinets, optical copies. Consideration must also be given to specialist recovery contracts. These are best negotiated at a corporate level ensuring the best value for money through economies of scale.
- **Power Supplies:** Uninterrupted Power Supply (UPS) and back-up generators are expensive. They are essential for the protection of Mission Critical Activities and their dependencies. As diesel fuel has a limited life there is a need to balance storage capacity/time against expenditure.
- **Sourcing:** The intra-organisation sourcing and outsourcing of Mission Critical Activities and their dependencies is a critical consideration and must be the subject of a rigorous process. More and more organisations are outsourcing Mission Critical Activities and their dependencies to create virtual organisations. It is critical to remember that the risk to the organisation's reputation and brand image cannot be shifted to either intra-organisation sourcing or outsourced providers. The risk always remains with the business.

Methodologies/Techniques.

The methods, tools and techniques to develop a Business Continuity Management Resource Recovery Plan include:

- Current state assessment 'Gap' analysis.
 - Questionnaire(s).
 - Scorecards.
 - Interviews (structured and unstructured).
- Stakeholder analysis.
- Scenario planning.
- Checklists.
- Workshops (facilitated by a professional BCM practitioner).
- Generic minimum standard plan format and contents that can be customised. This approach enables standardisation in plan production and terminology. Another key benefit is that common escalation processes can be defined for the organisation.
- A variety of business continuity planning and plan development software products are available but they are not essential to enable the successful development of a Business Continuity Plan. They can however provide significant benefits in the areas of plan maintenance and referential integrity.
- Business Continuity Management Solutions:
 - Work area Recovery.
 - IT Disaster Recovery(ITDR)
 - Data Recovery (all media)
 - Telecommunications Recovery.
 - Staff Relocation.
 - Ship-in-Services.
 - Damage Assessment.
 - Restoration.
 - Salvage.
 - Security.
 - Shared Services e.g. HR function.
- The comparison of requirements against potential solutions.
- Recovery resource profiling.
- End-to-End (E2E) service and product process mapping.
- Cost Benefit Analysis.
- 3rd party specialist suppliers.

- SWOT Analysis (Strengths, Weaknesses, Opportunities and Threats).
- Porter's Value Chain.

Process.

The professional BCM practitioner has a key role in the planning and development of a BCM Resource Recovery Plan. The professional BCM practitioners experience provides a valuable early 'reality' check in ensuring the plan is appropriate, practical and workable.

The key constructs of the BCM Resource Recovery Plan development and planning process include:

- Appoint a role to be accountable/responsible for the Business Continuity Plan.
- The outputs from the Business Impact Resource Recovery Analysis (BIRRA).
- Define the scope of the plan.
- Define the objectives of the plan.
- Develop and approve a BCM planning and plan development process and programme.
- Appoint a planning and plan development programme manager.
- Create a business continuity planning team (actual or virtual) to carryout the planning and develop the plan.
- Decide the structure, format, components and content of the plan.
- Determine the strategies on which the plan is based.
- Determine the key approaches to key phases of the plan.
- Conduct a BCM 'gap' analysis to establish the current state assessment.
- Gather information to populate the plan.
- Individuals nominated to fulfil roles within the plan.
- Draft the plan.
- Circulate the draft of the plan for consultation, review and challenge.
- Gather feedback from consultation, review and challenge process.
- Amend plan as appropriate.
- Plan agreed and 'signed-off' pre-exercising by role accountable/responsible for the plan.

- Ongoing 'due diligence' e.g. relationship management, exercising, rehearsal, testing and maintenance of plan to establish it is effective and fit-for purpose'.

Frequency and Triggers.

Whilst Business Continuity Management resource recovery solutions and their plans should be reviewed on an ongoing basis the frequency and triggers that determine when such a plan should be reviewed or audited 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 review or audit should be aligned with the review of other BCM related strategies, plans and solutions and be carried out at least every 6 months, unless:

- It is the initial development and documentation of the BCM Resource Recovery Plan.
- Where the pace of business change is particularly aggressive a more frequent review or audit 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.
 - BCM strategy and/or scope.
 - BCM solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation sourcing and/or outsourced providers)
 - Post BCM 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 or Accountable or should be either Consulted or Informed (RACI) in the planning and development of the Business Continuity Management resource recovery solutions and plans. 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 Management				
Operational Middle Management				
Operational Supervisors and Staff				
Professional BCM practitioner				
Legal				
Finance				
Telecommunications				
Technology				
Facilities/Property Management				
Human Resources.				
Suppliers of specialist BCM resources and services (intra-organisation and/or outsourced providers)				
Commercial Services Management				
Relationship Management				
Subject Experts (where appropriate)				
Suppliers of business services/products (intra-organisation and/or outsourced providers)				

Deliverables.

The deliverables of the Business Continuity Management resource recovery solutions and plans include:

A clearly defined and documented Business Continuity Management Resource Recovery Plan that is agreed and 'signed-off' by the organisation's executive/senior management and/or business unit manager.

Good Practice Evaluation Criteria.

The Good Practice evaluation criteria of a Business Continuity Management Resource Recovery Plan(s) includes:

BCM Solutions : General.

- Have the owners of the organisations Mission Critical Activities (MCA's) and dependencies developed and implemented BCM solutions within their BCM strategy/plan to achieve the RTO, RPO and LBC of their MCA's and dependencies?

- Has the suitability of alternate BCM solutions been fully assessed?
- Have the organisation's BCM resources been assigned/allocated according to Business Impact Analysis (BIA) results identifying Mission Critical Activities, their dependencies and single points of failure?
- Does the organisation have a clearly defined process to ensure that the learning points and/or recommendations arising from an exercising, rehearsal and testing programme and/or actual incidents (whether internally or externally) must be incorporated within the BCM resource recovery planning process?
- Does the organisation have a clearly defined process that must be employed to challenge and review the assumptions upon which the resource recovery strategy and plan is based?
- Are the Business Continuity Institute BCM Good Practice Guidelines used as a part of the Resource Recovery Solutions and Plans assurance process?
- Does the Resource Recovery Solutions and Plans process achieve the Resource Recovery Solutions and Plans outcomes set out in the Business Continuity Institute BCM Good Practice Guidelines?
- Does the Resource Recovery Solutions and Plans process provide the Resource and Recovery Solutions and Plans deliverables set out in the Business Continuity Institute BCM Good Practice Guidelines?

BCM Solutions : Insurance.

- Does the organisation consider insurance as its principal BCM solution?
- Does the organisation's insurance cover the cost of business interruption in your worst case scenario?
- Does the organisation's insurance cover the cost of equipment, including replacement values, in your worst case scenario?
- Does the organisation's insurance cover include additional operating costs in your worst case scenario?
- Does the organisation's insurance cover include financial loss (and its limitation) in your worst case scenario?
- Does the organisation's insurance cover include the cost of recreating systems and programme documentation in your worst case scenario?
- Does the organisation's insurance cover include the cost of restoring and/or recreating lost data in your worst case scenario?
- Are insurance coverage exclusions clearly defined and understood?
- Does the BCP provide a clearly defined insurance notification process?

- Are all BCM insurance policies and their coverage limits reviewed regularly for adequacy and cost benefit?
- Does the organisation involve loss adjusters in the BCM process as early as possible?

BCM Solutions : People.

- Does the BCP clearly identify key members of staff (skills, knowledge, organisational role and experience) to ensure BCM?
- Does the BCP clearly define a process/strategy to ensure the availability of identified key personnel and/or uniquely skilled staff?
- Does the BCP provide for the non-availability of key personnel?
- Does the BCP provide clearly defined process for relocating staff e.g. transportation and accommodation?
- Does the BCP take account of the possibility of transport disruption preventing key staff from being able to reach a work area recovery site?
- Does the BCP provide clearly defined and documented RTO and RPO objectives for personnel/staff recovery?
- Does the BCP provide an exercising programme for the recovery of MCA's and their support activities personnel?

BCM Solutions : Work Area Recovery (WAR).

- Has a work area recovery strategy for MCA's and their support activities been developed and documented within the BCP?
- Is the work area recovery site situated at least 800 metres (based on a large vehicle bomb) away so as not to be affected by the same incident/event/crisis?
- Has the quantity and configuration of work area recovery needed for MCA's and their dependencies been agreed; 'signed-off' by the business owner and clearly documented within the BCP?
- Is the level of specialist service support to enable the use of an alternate site (WAR) or other services clearly identified within a service contract or service level agreement (SLA)?
- Does the BCP provide clearly defined details and a process for work area recovery?
- Does the BCP provide clearly defined RTO and RPO objectives for work area recovery?
- Does the BCP provide a map/directions to the work area recovery relocation?

- Do key staff and managers know where the work area site is located and how to get there?
- Have alternative work area recovery facilities been sourced via an internal or a specialist (outsourced/contracted) supplier?
- Is the internal sourcing of work area recovery facilities contained within an SLA?
- Does the outsourcing of work area recovery facilities provide for dedicated (sole) use?
- Does the outsourcing of work area recovery facilities only provide for shared (first-come-first-served) use?
- If the organisation is using a syndicated third party work area recovery solution is it aware of the suppliers sales ratio and proximity policies?
- Does the contracted special service (outsourced) sourcing of work area recovery facilities comply with the organisations Resource Recovery Strategy?
- Is there a BCM battlebox at the work area recovery location?
- Does the BCP provide a clearly defined process to invoke the work area recovery solution?
- Has the work area recovery facility been evaluated based on predefined selection criteria?
- Does the BCP provide a clearly define minimum level of resource profile to continue MCA's and dependencies in a work area recovery environment?
- Does the work area BCM solution include and clearly define resource details concerning standard configured power supplies, type of lighting, air conditioning and other facility requirements for staff and equipment?
- Does the BCM work area recovery solution include and clearly define resource details concerning standard configured workstations?
- Does work area solution include and clearly define resource details concerning trading facilities?
- Does the BCP provide a testing programme for the recovery of MCA's and their dependency work area systems?
- Does the work area recovery facility have the necessary technology infrastructure e.g. telecommunications and IT to support the MCA's and their dependencies?

BCM Solutions : Information Technology.

- Has an Information Technology (IT) recovery strategy for MCA's and their dependencies been developed and documented within the BCP?

- Does the BCP clearly identify that the ITDR site is located at least 800 metres (based on a large vehicle bomb) from the site of the event?
- Does the BCP provide clearly defined details and a process for the restoration of technology i.e. IT/IS?
- Does the BCP provide a clearly defined and documented inventory of all IT systems software necessary for the BCM of MCA's and their dependencies to achieve their BCM RTO and RPO objectives?
- Has the configuration of IT needed for MCA's and their dependencies been agreed; 'signed-off' by the business owner and clearly defined within the BCP?
- Does the BCP provide clearly defined details and a process to ensure the availability of critical IT resources at short notice?
- Does the business area have a process to ensure that all technology solutions are compliant with the Organisation IT security architecture?
- Does the BCP provide clearly defined RTO, RPO and LBC objectives for IT recovery?
- Does the inventory of resources necessary to recover MCA's and their dependencies include CPU's disk drives, tape drives, servers and printers?
- Have alternative facilities (IT DR) for the recovery of IT for MCA's and their dependencies been identified and subject to an SLA or contract?
- Does the BCP provide a testing programme for the recovery of the IT systems of MCA's and their dependencies?
- Have the business owners of the MCA's and specialist third party service providers been involved in the actual testing of the recovery of the IT support systems?
- Does the BCP provide clear details and process for the recovery of critical application for MCA's and their support activities?
- Does the BCP provide a testing programme for the recovery of critical applications of MCA's and their dependencies?
- Have the business owners of the MCA's and specialist third-party service providers been involved in the actual testing of the recovery of the MCA's critical applications?

BCM Solutions : IT Software.

- Does the BCP provide a clear inventory of all IT systems software necessary for the BCM of MCA's and their support services to achieve their BCM RTO, RPO and LBC objectives?
- Has the configuration of IT software systems needed for MCA's and their dependencies been clearly defined been agreed and 'signed-off' by the business owner?

- Does the BCP provide clear details and a process for the restoration of IT systems software?
- Does the BCP provide clear details of specialist software configuration(s) and a process for their restoration?
- Does the inventory of resources necessary to recover MCA's and their dependencies include configurations e.g. operating systems, DBMS?
- Does the inventory of resources necessary to recover MCA's and their dependencies include versions and dates of last update?
- Does the inventory of resources necessary to recover MCA's and their dependencies include security software needed to ensure protection and control of data access paths throughout the continuity process?
- Does the BCP provide a testing programme for the recovery of MCA's and their dependencies IT software systems?
- Have the business owners of the MCA's and specialist third party service providers been involved in the actual testing of the recovery of the IT software systems?
- Is a copy of software licences kept 'off-site'?

BCM Solutions : Telecommunications.

- Has a telecommunications recovery strategy for MCA's and their dependencies been developed and clearly defined within the BCP?
- Has an inventory and configuration of telecommunication needed for MCA's and their dependencies been agreed; 'signed-off' by the business owner and clearly defined within the BCP?
- Does the BCP provide clearly defined RTO, RPO and LBC objectives for telecommunication recovery?
- Does the BCP provide clear details and a process for the restoration of telecommunications?
- Does the BCM telecommunications inventory include details of modems, communication lines and switching equipment?
- Does the BCM telecommunications solution provide for 'ship in' telecommunication services?
- Does the BCM telecommunications inventory include and clearly define details of voice and data lines?
- Does the BCM telecommunications inventory include and clearly define details of descriptions of speed, frequency bandwidth and circuit identification number of communication channels?

- Have alternative facilities for the recovery of telecommunications for MCA's and their support activities been identified and subject to an SLA or contract?

BCM Solutions : Data.

- Does the Organisation have clearly defined backup procedures for all applications (including standalone PC's and laptops) and data (both electronic and paper e.g. vital/unique records/documents) necessary to support MCA's and their dependencies?
- Does the BCP provide a clearly defined process for the off-site storage (at least 800 metres from the data source – this is based on a large vehicle bomb) of backup data (both electronic and paper) necessary to support MCA's and their dependencies?
- Have off-site storage sites been sourced via a specialist (outsourced/contracted) supplier?
- Have off-site storage sites been sourced via an intra-organisation supplier?
- Is the sourcing of off-site storage clearly defined within a contract and/or SLA?
- Does the Organisation have clearly defined recovery and restoration process and procedures in place for all data (both electronic and paper e.g. vital and unique records/documents) necessary to support MCA's and their dependencies?
- Does the BCP provide clearly defined RTO, RPO and LBC objectives for the recovery and restoration of data (both paper and electronic mediums) necessary to support MCA's and their dependencies?
- Does the BCP provide a testing programme for the recovery and restoration of data (both electronic and paper) necessary to support MCA's and their dependencies?
- Have the business owners of the MCA's, work area recovery provider and specialist third-party data storage provider been involved in the actual testing of the recovery and restoration of data (both electronic and paper) necessary to support MCA's and their dependencies?
- Can critical data (both electronic and paper) necessary to support MCA's and their dependencies be recovered simultaneously at more than one work area recovery site if required?
- Does the organisation have a clearly defined process for storing critical papers and other work-in-progress e.g. in pre-identified fireproof cabinets?
- Does the organisation have a clearly defined document management and secure storage process for critical/unique documents e.g. deeds, or other items?

BCM Solutions : Equipment.

- Does the BCP provide clear details and a process for the obtaining of support equipment e.g. photocopier?

- Has the configuration of equipment needed for MCA's and their dependencies been agreed; 'signed-off' by the business owner and clearly documented within the BCP?

BCM Solutions : BCM Service Providers.

- Is the level of specialist BCM service(s) to enable the use of an alternate (recovery) site or other services clearly identified and documented within the service contract and/or SLA and a copy placed in the BCP?
- Does the BCP provide clear details and a process for the initiation and progressing of recovery, restoration and salvage service by specialist BCM service(s) suppliers?
- Does the BCP provide clear details and a process for the salvage, cleanup and rebuilding of the primary site?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and salvage contract or SLA clearly identify and define the duration of the agreement?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define a schedule of IT hardware, peripherals and functionality that will provided?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the operating systems, data and specialist programmes that will be provided?
- Does the specialist BCM service(s) support e.g. work area recovery, telecommunications recovery and restoration contract or SLA clearly identify and define the telecommunications resources and functionality that will be provided?
- Does the BCM service(s) support e.g. work area recovery, IT, telecommunications and data recovery and restoration contract or SLA clearly identify and define the level and duration of technical support that will be provided?
- Does the BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the office/workspace provided?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the amount of testing time available?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the security provision?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the invocation process?
- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define the annual fee, invocation and variable costs?

- Does the specialist BCM service(s) support e.g. work area recovery, IT recovery and restoration contract or SLA clearly identify and define alternate arrangements if the site, resources or service is not available?

BCM Solutions : Business Services.

- Does the BCP provide clear details and a process for the delivery and collection of mail at the primary site or work area recovery site?
- Has a current list of key service providers, suppliers and other third-party sourcing contacts been identified and documented within the BCP?
- Does the BCP provide clear details of the solutions i.e. power generators, in the event of an electricity outage?
- Does the BCP provide clear details of the Uninterrupted Power Supply (UPS) in the event of a power outage?

BCM Solutions : Security.

- Do the BCM solutions within the BCP have appropriate physical security and environmental controls?

BCM Solutions : Business Processes.

- Does the BCP provide clear details and a process for recovering MCA work-in-progress?
- Does the BCP provide clear details and a process concerning work backlog processing?
- Does the BCP provide clear details and a process for the provision of manual operations and fallback solutions and related activities to achieve MCA's RTO and RPO wherever gaps exist between IT recovery capabilities and BCM needs?

BCM Solutions : Change Management.

- Does the BCP provide clear change management controls for BCM solutions (in particular telecommunications, work area recovery and ITDR)?
- Does the organisation have a clearly defined change control process to ensure BCM requirements and selected BCM solutions are maintained in an up-to-date and fit-for-purpose status?

BCM Solutions : Sourcing (inc' intra-organisation sourcing and outsourcing).

- Does the Organisation maintain a schedule of its sourced (intra-organisation and/or outsourced provider) Mission Critical Activities their dependencies and single points of failure?

- Does the Organisation's Sourcing Policy clearly define that an outsourced or inter-organisation sourcing service provider of a Mission Critical Activities and/or their dependencies must have a verifiable, fit-for-purpose and demonstrated BCM capability?
- Does the organisation have a clearly defined 'due diligence process' to verify and validate that an outsourced or inter-organisation sourcing service provider of Mission Critical Activities and/or their dependencies has a fit-for-purpose and demonstrated BCM capability in respect of each Mission Critical Activity and dependencies?
- Does the business owner of each of the organisations Mission Critical Activities and/or their dependencies provide a 'signed off' contract/service level agreement BCM compliance (due diligence) review and challenge report of the BCM capability of the sourcing provider(s)?
- Does the organisation have a clearly defined and documented governance structure to relationship manage any ongoing and/or actual sourcing of its Mission Critical Activities and/or their dependencies?
- Does the organisation have a sourcing exit strategy/plan i.e. either switch the activity or dependency to another outsourcer or intra-organisation provision to cover the complete failure of any contract or service level agreement for each of its outsourced Mission Critical Activities and/or their dependencies?
- Has the organisation verified that its sourcing (intra-organisation and/or outsource provider) exit strategy/plan is capable of achieving the BCM RTO, RPO and LBC of the impacted Mission Critical Activities and/or their dependencies by testing or invocation?
- Does the organisation have an effective communication process with its sourcing providers (intra-organisation and/or outsourced) to provide immediate notification of an event/incident causing, or likely to cause, interruption, disruption or loss of a sourced Mission Critical Activity and/or their dependencies?
- Is a formal BCM schedule that clearly defines the minimum Level of Business Continuity (LBC) requirements incorporated into the sourcing contract and/or service level agreement of each of the organisation's sourced Mission Critical Activities and/or their dependencies?
- Does the organisation have clearly defined BCM compliance (due diligence) review and challenge process concerning the resilience of the sourcing of its Mission Critical Activities and/or their dependencies?
- Does the business owner of each of the organisations Mission Critical Activities and/or their dependencies provide a 'signed off' contract/service level agreement BCM compliance (due diligence) review and challenge report of the resilience of its sourcing arrangements?
- Does the organisation have a clearly defined and documented process whereby the owner of a Mission Critical Activity and/or dependency(ies) formally accepts any residual risk from their sourcing as identified by a formal Business Impact Analysis and Risk Assessment?

- Is the risk of sourcing Mission Critical Activities and/or their dependencies a part of the organisations ongoing business risk assessment, profile and appetite?
- Does the sourcing contract and/or service level agreement of the organisation's sourced Mission Critical Activities and their dependencies include a right by the organisation to audit the BCM capability and resilience of the sourcing provider against predefined and agreed BCM standards e.g. within RTO, RPO and to the minimum Level of Business Continuity (LBC)?
- As a part of the organisations due diligence process of the sourcing of its Mission Critical Activities and/or their dependencies does the organisation regularly receive certified copies of the sourcing supplier's own internal BCM exercising reports and action plans?
- Does the organisation's sourcing process clearly define that a BCM professional practitioner must be engaged at the inception of all projects and included in sourcing decisions of Mission Critical Activities and their dependencies?
- Does the organisation's BCP clearly identify that sourcing providers will be expected to assist via their best endeavours to provide assistance in the organisations BCM process?

Further Reading.

- Birch, D. (2002) 'Business Continuity for telecommunications', *Continuity*, Vol.6, No.1, pp.10-13.
- Business Continuity Institute (1999) 'Benchmarking Business Continuity Management', BCI, Worcester.
- Business Continuity Institute (2000) 'The ten competencies of Business Continuity Management', BCI, Worcester.
- Business Continuity Institute (2001) 'Getting started', BCI, 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.
- 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 Reserve Bank, (2002) 'Implications of 9/11 for the financial services sector', *Bank of International Settlement Review*, pp.1-5.
- Ferguson, R.W. (2002) 'A supervisory perspective on disaster recovery and business continuity', *Bank of International Settlement Review*, pp.1-4.
- 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', FSA, London, pp.1-19.
- Financial Services Authority. (2002) ' FSA working paper on Business Continuity Management', FSA, London, pp.1-20..
- Frost, C. (1994) 'Effective responses for proactive enterprises: Business continuity planning', Disaster Prevention and Management, Vol.3, No.1, pp.7-15.
- Halford, P. (2001), 'Addressing business continuity management', Risk Management, Vol.6, No.1, pp.21-23.
- Home Office. (1996) ' How resilient is your business to disaster', HMSO, London.
- Honour, D. (2001) 'Heeding the lessons of 9/11', International Journal of Business Continuity Management, Vol.2, No.1, pp.13-17.
- Kirvan, P.F. (2000) 'Business continuity strategies for call centres', Continuity, Vol.4, No.2, pp.9-10.
- Moore, P. (2001) 'Ensuring business continuity for vital business systems', Risk Management, Vol.6, No.1, pp.29-31.
- Porter, M.E. (1985) 'Competitive Advantage: Creating and sustaining superior performance', Free Press, New York.
- Power, P. (1999) 'Business Continuity Management: Preventing chaos in a disaster', Department of Trade and Industry, London.

Videos.

British Council for Shopping Centres (1999) 'Shopping Centre Bomb Threats', Williams Management Communication, London.

British Telecommunications (1995) 'The Foresight Saga: Planning for Continuity of Communications', British Telecommunications Plc, London.

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

Royal and Sunalliance (1996) 'The Manchester Bombing Incident', Elite Television, Leeds.

Case Studies.

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

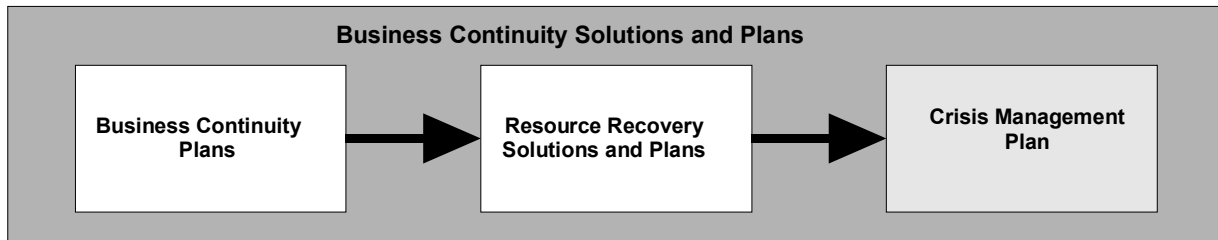
Honour, D. (2001) 'Heeding the lessons of 9/11', International Journal of Business Continuity Management, Vol.2, Issue.1, pp.13-17.

Manchester Bombing in 1996 in HMSO (1999) ' Business As Usual - Maximising business resilience to terrorist bombings', pp.6-10.

Mellish, S. (2000) 'When a BCP really comes into its own', Continuity, Vol.4, Issue4, pp.4-6.

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

Crisis Management Plan.



Introduction.

Crisis management is linked to corporate governance and the importance of an effective crisis management capability was recently reinforced by the unmitigated and tragic terrorist attack at the World Trade Centre in New York (9/11). The ability to achieve effective crisis management and business continuity during a time of crisis involves strong leadership and co-ordination between the people responsible individual site/building and business crisis management. In addition to the benefits of the crisis management planning and exercising process a critical part of an organisation's crisis capability is frequently overlooked. It concerns the team working, commitment, competence and confidence of the people and roles that are required to manage a crisis.

The consequences of not achieving an effective and fit-for-purpose crisis management capability will expose an organisation's brand to unnecessary financial, credit, reputation, regulatory, legal, market and operational risk.

Purpose.

The purpose of a Crisis Management Plan (CMP) is to provide an effective, fit-for-purpose predefined and documented framework and process to enable an organisation to manage effectively a crisis event whether of a physical e.g. site or non-physical e.g. reputation/brand or security e.g. kidnap/burglary nature.

Outcomes.

The outcomes of a Crisis Management Plan include:

- A clearly defined and documented Crisis Management Plan to support the role of the organisation's Crisis Management Team during a crisis event.
- Maximisation of the organisation's reputation and brand image.
- Maintenance of public, stakeholder, market and regulatory confidence and trust.
- Demonstrate effective and fit-for-purpose crisis management and governance to the media, markets, customers, stakeholders and regulators.
- Limiting/preventing the impact of a crisis event.

- Minimising the impact of crises on the organisation's stakeholders by providing continuity of services, products and resources.
- The establishment of a clearly predefined and documented Crisis Management response following a business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed.
- Compliance with legal requirements.
- Compliance with regulatory requirements.
- A demonstration to stakeholders that the organisation has a BCM capability.
- A clearly defined and documented owner of the Crisis Management Plan.
- Clearly defined Crisis Management roles, accountability, responsibility and authority
- A clear demonstration to stakeholders and the market that the organisation has a Crisis Management capability.

Components.

This section of the guidelines sets out the minimum standard of components and their content for a Crisis Management Plan. It is not intended to provide an exhaustive list to cover every eventuality, as by their nature all crises are different. If the minimum standard is considered insufficient to meet the needs of an organisation the additional requirements should be added to the Crisis Management Plan. The high level contents of a Crisis Management Plan will vary from organisation to organisation and will naturally reflect the organisational structure.

The structure (running order of the table of contents) of the plan should also be customised to meet the specific needs of an organisation. Whilst a plan structure is not mandated it is recommended that a standard format be adopted to enable consistent application across an organisation.

Good practice identifies that a Crisis Management Plan should be modular in design with different consecutively numbered/named sections. The different sections provide an opportunity to form separate documents (modules) that can be supplied to individuals and/or teams on a need to know basis. There must be a clearly defined and documented control and change management process. The pagination of each section also provides for ease of reference. A further method is the production of the different modules and team plan on different coloured paper to provide ease of use and reference at the time of a crisis.

The components of a Crisis Management Plan include:

HEADER:

- Document classification (e.g. company confidential as per the organisation's classification policy).

FOOTER:

- Version control reference (including date).
- Page number.

FRONT PAGE:

- Title.
- Document classification e.g. company confidential as per the organisation's classification policy.
- Version control i.e. version number, date, change author and change details.
- Management 'sign-off' of plan.

DISTRIBUTION LIST.**TABLE OF CONTENTS.****SECTION 1: PLAN OVERVIEW.**

- Introduction.
- Purpose (Aim) of plan.
- Scope.
- Objectives.
- Assumptions.
- Plan ownership
- Crisis Management Levels and Escalation
- Crisis Management Process Flowchart (copy contained with Appendices)
- Evaluation and categorisation framework (copy contained within Appendices)

SECTION 2: EMERGENCY PROCEDURES (Site Plans only).

- Building Evacuation i.e. reference where they can be found.
- Invacuation (if building previously surveyed and appropriate location identified) i.e. reference where they can be found.
- Bomb Threat and similar scenarios i.e. reference where they can be found.
- Evacuation points (including alternate or off-site).
- Dispersal of staff and visitors.

SECTION 3: ROLES, ACCOUNTABILITY, RESPONSIBILITIES AND AUTHORITY

A crisis management team and its composition may vary in size throughout a crisis based on the circumstances of the crisis and the level of, skills, knowledge and expertise required to manage it and its resolution. This may include internal and external individuals and/or organisations.

CRISIS MANAGEMENT ACCOUNTABLE EXECUTIVE.**Role:**

The role of the Crisis Management Accountable Executive is to take overall ownership for the management of the crisis as a whole. The following list of key responsibilities should not be seen as exhaustive or restrictive.

Responsibilities:

- Overall responsibility and governance for the management of the crisis.
- Notification and updates to the organisation (as appropriate).
- Representation at organisational (corporate) level steering committee (where appropriate).
- Escalation to organisational (corporate) level crisis management status.
- Ensure the implementation of the organisation's crisis management framework.
- Appoint members of the crisis management steering committee.
- Appoint a crisis manager.
- Chair of the crisis management steering committee.

CRISIS MANAGEMENT STEERING COMMITTEE.**Role:**

The role of the Crisis Management Steering Committee is to provide strategic direction for the management of the Crisis. The following list of key responsibilities should not be seen as restrictive or exhaustive:

Responsibilities:

- Implement and manage the crisis management plan.
- On-going review of crisis information, decisions and actions taken.
- Provide the crisis management strategy and decision making.
- Ensure the implementation of the organisation's crisis management framework.
- The provision of appropriate levels of skills and resources to implement the crisis management strategy and tactics.
- Management of external communications (**following consultation with the organisation's Corporate Communications and Public Relations function**).
- Inform and liaise with regulatory authorities (**following consultation with the organisation's legal and compliance functions**).
- Where necessary prioritise the allocation of resources between business areas
- Agree business priorities.
- Maintain an accurate crisis management steering committee strategy and decision log throughout the incident.

CRISIS MANAGER.**Role:**

The role of the Crisis Manager is to take ownership for the implementation of the crisis management steering committee strategy, decisions and any appropriate plans. The following list of key responsibilities should not be seen as exhaustive or restrictive.

Responsibilities:

- Clear authority to manage the Command and Co-ordination of the implementation of the organisation's Crisis Management Plan.
- Pre-incident nomination of Crisis Management Team(s).

- Pre-incident nomination of Crisis Management Support/Logistics Team.
- Identify and appoint appropriate persons/roles to the Crisis Management Team
- The provision and implementation of tactical (remedial) action plan(s) to implement crisis management steering committee strategy, decisions and any appropriate plans.
- The provision of a Crisis Command Centre and alternate.
- On-going review of crisis information, decisions and actions taken.
- Co-ordination of business streams (where appropriate).
- Nominate the Crisis Command Centre.
- Crisis scenario planning and provision of remedial, contingency and business continuity action plans.
- Ensure the implementation of the Group Incident Management Framework Exec responsibility?
- Report to the Crisis Management Steering Group.
- To ensure the maintenance of an accurate crisis management team decision and action log throughout the incident.
- Maintain an effective and efficient 'fit for purpose' Crisis Management Plan capability.
- Invocation of the Crisis Management Plan.
- Prioritise resource allocation when issues of conflict arise.
- Authorise appropriate and necessary expenditure.
- Management of allocated financial and other resources.
- Liaison with affected business areas and keep them advised of the situation via status reports.
- Media and press in liaison with the organisation's Corporate Communications and Public Relations.
- To ensure (where necessary) all statutory and regulatory authorities/bodies are informed following consultation with the organisation's compliance and legal functions.

CRISIS MANAGEMENT TEAM.

Role:

The role of the Crisis Management Team is to provide an effective and efficient 'fit for purpose' operational crisis management capability to implement the Crisis Management Steering Committee strategy, decisions and any appropriate plans. The following list of key responsibilities should not be seen as exhaustive or restrictive.

Responsibilities:

- Provide an effective 'fit-for-purpose' crisis management infrastructure.
- Support the Crisis Manager in the implementation of tactics to implement the Crisis Management Steering Committee strategy, decisions and any appropriate plans.
- Maintain an audit/review of crisis information and appropriateness of tactical decisions and actions taken.
- Staff the nominated Crisis Management Command and Co-ordination Centre.
- Monitor and maintain Crisis Management Action/Task Status Report(s).
- Ensure the implementation of the organisation's crisis management framework.
- The maintenance of an accurate Crisis Management Team decision and action log.
- Provide on-going crisis status reports concerning:

- Casualties and Fatalities.
- Damage Assessment.
- Salvage.
- Security - Physical and Information.
- Media - Interest and lines of enquiry.
- Statutory and Regulatory Bodies.
- Operation of Technology and Communication Infrastructure.

If the crisis requires contact with regulatory bodies; legal or media advice, this team must either include representatives from the legal, corporate communications and/or compliance teams or liaise closely with them prior to any steps being taken or contact being made in those areas.

CRISIS MANAGEMENT SUPPORT/LOGISTICS TEAM.

Role:

The role of the Crisis Management Support/Logistics Team is to provide support and logistics for both the Crisis Management Steering Committee and Crisis Management Team. The following list of key responsibilities should not be seen as exhaustive or restrictive.

Responsibilities:

- Set-up and maintain the nominated Crisis Management Command Centre
- Provide the appropriate level of support, resources and logistics to enable the functioning of the Crisis Management Steering Committee and Crisis Management Team.

SITE BUSINESS CONTINUITY MANAGEMENT CO-ORDINATOR.

Role:

The role of the Site Business Continuity Management Co-ordinator occurs where large “campus” sites require co-ordination across different business areas. Each business area nominates its own Site BCM Co-ordinator. The role requires the nominated individual to use their business knowledge, experience and expertise to co-ordinate the business continuity efforts of their on-site business units in liaison with the individual business unit managers and the Site Crisis Management Team.

Responsibilities:

- Monitor the implementation of the organisation’s BCM Policy in respect of their on-site business units.
- Co-ordinate and prioritise their on-site business units BCM recovery activity.
- To liaise with the managers of their on-site business units to ensure that their telephony and technology recovery requirements are clearly defined documented, agreed and ‘signed-off’ by their sourcing supplier(s).
- Provide and maintain a prioritised BCM recovery profile of their on-site business units e.g. recovery location and contact details, recovery time objective and recovery point objective.
- Maintain a list of contact points for their on-site business units and escalation within their business area.

- Co-ordination and prioritisation of the BCM recovery across their site in liaison with the nominated Site BCM Co-ordinators of other business areas.
- Liaise with the manager of each of their on-site business units to establish each has an exercised and 'fit for purpose' business continuity plan and capability based on an up-to-date Business Impact Analysis.
- Advise their business area and the Site Crisis Management Team of the business continuity status of their on-site business units throughout the crisis taking into account any decisions taken by the Site Crisis Manager in respect of staff safety and the site as a whole.
- Liaise with the manager of each of their on-site business units to establish that the manager has briefed all their staff so that they are aware of their roles and responsibilities and know what to do if their business continuity plan is invoked.

SECTION 4: NOTIFICATION, INVOCATION AND ESCALATION.

- Notification process and/or flowchart.
- Invocation process and/or flowchart.
- Escalation process and/or flowchart.
- Call out/information (call tree) cascade process and/or flowchart (copy located within Appendices).

SECTION 5: CRISIS MANAGEMENT TEAMS.

- Membership of Crisis Management Steering Committee and alternates.
- Designated Crisis Management Team Manager and alternates.
- Membership of Crisis Management Team and alternates.
- Membership of Crisis Management Logistics Team and alternates.

SECTION 6: COMMAND CENTRE(S).

- Location and contact details of 'on-site' and 'off-site' command centres (including non-city or metropolitan areas where appropriate).
- Map and directions to 'off-site' command centre location.
- Command centre resource profile.
- Battlebox.

SECTION 7: CONTACTS.

- External.
- Internal.
- Subject Experts e.g. product, service, system.

SECTION 8: TASK CHECKLIST(S) AND AIDE MEMOIRES.

- Mandatory tasks.
- Discretionary tasks.
- Task completion tracking process.
- Across the organisation's business areas (where appropriate).

SECTION 9: SUPPORTING INFORMATION.

- Injuries and fatalities.
- Staff welfare and counselling.
- Media and public relations.
- Emergency Services and Local Authority (Site Plan only).
- Health and Safety.
- Finance.
- Legal Advice (include Legal Privilege).
- Insurance.
- Invocation of specialist Crisis/Business Continuity Management services (intra-organisation or external provider).
- Communications e.g. free-phone.
- Physical Security (Site Plan only).
- Business Unit Relocation Profile (Site Plan only).
- Schedule of Critical Business Activities or support activities (Business Area and Site Plan only)
- Internal briefings (preformatted agenda located with Section 10: Forms).

SECTION 10: FORM TEMPLATES.

- Evaluation and categorisation.
- Meetings agenda.
- Internal briefings.
- Crisis decision and action log.
- Crisis task list status report.
- Telephone message.
- Action or task worksheet.
- Incident Command Sheets (ICS)

APPENDICES:

- Contracts and Service Level Agreements.
- Evaluation Categorisation Framework.

Methodologies/Techniques.

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

- Current state assessment 'Gap' analysis.
 - Questionnaire(s).
 - Scorecards.
 - Interviews (structured and unstructured).
- Stakeholder analysis.
- Scenario planning.
- Checklist(s).
- Aide Memoire(s).

- Workshops (facilitated by a professional BCM practitioner).
- Generic minimum standard plan format and contents that can be customised. This approach enables standardisation in plan production and terminology. Another key benefit is that common escalation processes can be defined for the organisation.
- A variety of crisis management planning and plan development software products are available but are not essential to enable the successful development of a Crisis Management Plan. They can however provide significant benefits in the areas of plan maintenance and referential integrity.

Process.

The BCM professional has a key role in the planning and development of a Crisis Management Plan. The professional BCM practitioner's experience provides a valuable early 'reality' check in ensuring the Crisis Management Plan is appropriate, practical and workable.

The key constructs of the Crisis Management planning and plan development process include:

- Appoint a role to be accountable/responsible for the Crisis Management Plan.
- Define the scope of the plan.
- Define the objectives of the plan.
- Develop and approve a Crisis Management planning and plan development process and programme.
- Appoint a planning and plan development programme manager.
- Create a crisis management planning team (actual or virtual) to carry out the planning and develop the plan.
- Decide the structure, format, components and content of the plan.
- Determine the strategies on which the plan is based.
- Determine the key approaches to key phases of the plan.
- Conduct a crisis management 'gap' analysis to establish the current state assessment.
- Gather information to populate the plan.
- Individuals nominated to fulfil roles within the plan.
- Draft the plan.
- Circulate the draft of the plan for consultation, review and challenge.

- Gather feedback from consultation, review and challenge process.
- Amend plan as appropriate.
- Plan agreed and 'signed-off' pre-exercising by role accountable/responsible for the plan.
- Ongoing exercising, rehearsal, testing and maintenance of the plan to establish it is effective and fit for purpose.

Frequency and Triggers.

Whilst the organisation's Crisis Management Plan should be reviewed on an ongoing basis the frequency and triggers that determine when the plan should be reviewed or audited 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 review or audit should be aligned with the review of other BCM and Crisis Management related strategies, plans and solutions and be carried out at least every 6 months, unless:

- It is the initial development and documentation of the organisation's Crisis Management Plan.
- Where the pace of business change is particularly aggressive a more frequent review or audit 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.
 - BCM strategy and/or scope.
 - BCM solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation sourcing and/or outsourced providers)
 - Post BCM 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 or Accountable or should be either Consulted or Informed (RACI) in the planning and development of the organisation's Crisis Management Plan.

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 Management.				
Operational Middle Management.				
Operational Supervisors and Staff.				
Professional BCM practitioner.				
Site/Building/Business BCM Co-ordinator.				
Role(s) nominated as Crisis Manager(s) and alternates.				
Role(s) nominated as Crisis Team(s) Leader(s) and alternates.				
Role(s) nominated as Crisis Team(s) Member(s) and alternates.				
Legal.				
Regulatory.				
Finance.				
Telecommunications.				
Technology.				
Facilities/Property Management.				
Human Resources.				
Suppliers of specialist BCM resources and services (intra-organisation and/or outsourced providers).				
Emergency Services (where appropriate).				
Police (criminal issues).				
Local Authority Emergency Planning Officer (where appropriate).				
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/Outcomes.

The deliverables of the planning and development of the Crisis Management Plan include:

- A clearly defined and documented Crisis Management Plan that is agreed and ‘signed-off’ by the organisation’s executive/senior management.

Good Practice Evaluation Criteria.

The Good Practice evaluation criteria of the organisation’s Crisis Management Plan include:

Crisis Management Planning.

- Does the organisation have a clearly defined and documented crisis management policy?
- Does the organisation have a clearly defined and documented crisis management framework?
- Does the organisation's planning process clearly identify, address and comply with current regulatory requirements?
- Does the organisation's planning process clearly identify, address and comply with current legal requirements?
- Does the organisation's planning process clearly identify, address and comply with the organisation's current crisis management policy?
- Does the organisation's planning process incorporate worst case 'Scenario Planning'?
- Does the organisation's planning process incorporate the use of 'Fault Tree' analysis?
- Does the organisation's planning process incorporate the use of 'Event Tree' analysis?
- Does the organisation's planning process incorporate the use of stakeholder analysis?
- Does the organisation's planning process clearly identify and address insurance issues?
- Is the organisation's planning process co-ordinated with organisation sourcing (outsourcing and intra-organisation sourcing) service providers?
- Is the organisation's planning process co-ordinated with other parts of the organisation e.g. geographically/departments/sites?
- Do organisational managers fully understand their role in the crisis management planning process?
- Are templates/frameworks/sample crisis plans available for reference and to provide a standardised approach?
- Are professionally qualified Crisis Management practitioners involved in the planning process?
- Does the organisation's crisis management planning process incorporate the allocation of resources and finance as a part of the annual budget development and management process?
- Is the organisation's crisis management plan(s) reviewed by the organisation's legal department/representative as a part of the planning process?
- Have statutory/regulatory/official agencies been identified and included in the organisation's crisis management planning process?

- Have the emergency services and local authority been consulted in the development of the organisation's crisis management strategy(ies) and plan(s)?
- Does the organisation have a clearly defined process to ensure that the learning points and/or recommendations arising from an exercising, rehearsal and testing programme and/or actual incidents (whether internally or externally) must be incorporated within the crisis management planning process?
- Does the organisation have a clearly defined process that must be employed to challenge and review the assumptions upon which the crisis management strategy and plan is based?
- Are the Business Continuity Institute BCM Good Practice Guidelines used as a part of the Crisis Management assurance process?
- Does the Crisis Management process achieve the Crisis Management outcomes set out in the Business Continuity Institute BCM Good Practice Guidelines?
- Does the Crisis Management process provide the Crisis Management deliverables set out in the Business Continuity Institute BCM Good Practice Guidelines?

Crisis Management Plans.

- Does the Organisation have a clearly defined, up-to-date and fit-for-purpose Crisis Management Plan (CMP)?
- Does the CMP have a dated and 'signed-off' declaration by the accountable owner of the plan that it is fit-for-purpose and up-to-date?
- Does the CMP clearly establish and identify the accountable owner of the plan?
- Does the CMP clearly the role of the accountable owner of the plan?
- Does the CMP clearly identify and define the role that is accountable and/or responsible for its maintenance?
- Does the CMP clearly identify that it is an organisation confidential document?
- Does the CMP clearly indicate that it should not be disclosed outside the organisation without written authority of the plan owner?
- Does the CMP provide a clearly defined process for the independent review/audit of the plan at specific periods within the planning lifecycle?
- Do all CMP's within the organisation follow an integrated and agreed structure and minimum standard content?
- Does the CMP reflect the current BCI BCM Good Practice Guidelines?
- Does the CMP provide and define clear aims (purpose) and objectives?

- Does the CMP clearly identify and define the scope of the plan?
- Does the CMP contain a formal introduction?
- Does the CMP contain clear instructions on how to use the plan?
- Does the CMP contain clear details of how the plan is organised/structured?
- Does the CMP contain details of any assumptions either in its preparation or operation?
- Does the CMP contain a diagram of the organisation's crisis management operational structure and framework?
- Does the CMP have a comprehensive Table of Contents?
- Does the CMP include a distribution list?
- Does the CMP contain a glossary of terms?
- Does the CMP contain a clear instruction that a copy of the plan is kept at both an on-site and off-site location?
- Does the CMP provide a clear timeframe schedule of the minimum resource requirements to create a crisis command and control centre?
- Is the distribution of the CMP strictly controlled e.g. numbered copies?
- Does the CMP have change and version control procedures to maintain the integrity of the plan?
- Does the CMP clearly identify that it is an organisation confidential document?
- Does the CMP clearly identify that the document shall not be used by other than authorised employees not shall it be used or disclosed outside the organisation without authority?
- Does the CMP clearly identify and define a minimum exercising, rehearsal and testing programme to be completed within mandatory timescales?

Emergency Procedures.

- Does the CMP clearly set out and document emergency evacuation procedures; other staff and building safety procedures; evacuation and assembly points for different types of incident e.g. fire/bomb and their testing programme?
- Does the CMP clearly indicate that the protection of staff and other persons is the key priority in emergency procedures?

- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning disabled staff or visitors?
- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning the dispersal of staff, contractors or visitors?
- Does the site/building have a tannoy system to enable instructions/information to be communicated in a timely manner?
- Does the CMP clearly define the role, accountability, responsibility and authority of fire marshals and any other persons involved in emergency procedures?
- Are the site/building emergency evacuation procedures rehearsed regularly e.g. at least once per month?
- Are the site/building emergency procedures integrated with the requirements of the Local Authority?
- Does the BCP provide a clearly defined process for the application of containment measures in respect of damage and the overall impact of the crisis?
- Does the CMP provide a clearly defined process and criteria to classify any damage and the overall impact of the crisis?
- Does the CMP provide a clearly defined process to ensure there are proactive links to other organisations e.g. emergency services, suppliers that may be involved in the crisis management process?

Command and Control.

- Does the CMP provide a clearly defined Command and Control organisation structure to manage the crisis?
- Does the CMP provide clearly defined details of the primary and secondary Command Centre locations?
- Does the CMP provide clear details and/or a map of how to get to each Command Centre?
- Does the CMP provide a clearly defined process for invoking, operating and closing the Command Centre?
- Does the CMP provide a clearly defined operational structure and administration system for the Command Centre?
- Does the CMP provide clearly defined details of medical care, catering, accommodation and toilet facilities for the Command Centre?
- Does the CMP provide clearly defined details of a logistics/support team whose role is to set-up and maintain the Command Centre?

- Does the CMP provide a clearly defined Command Centre operational resource profile e.g. telephones?
- Has the effective capability of the Command Centre(s) been demonstrated and proven via exercising and/or invocation?

Notification, Invocation and Escalation.

- Does the CMP have a structured up-to-date and fit-for-purpose crisis notification, invocation and escalation process?
- Does the CMP contain clearly defined instructions as to whom has the authority to invoke (other than where it is self-evident) the plan?
- Does the CMP contain a clearly defined notification, invocation and escalation process flowchart?
- Does the CMP contain a clearly defined, up-to-date and auditable call-out (call tree) cascade process?
- Does the CMP contain a clearly defined up-to-date call-out (call tree) cascade process flowchart?
- Does the CMP contain a clearly defined, up-to-date and auditable information cascade process?
- Does the CMP contain a clearly defined, up-to-date information cascade process flowchart?
- Does the CMP contain clearly defined process for notifying the organisation's legal department/representatives?
- Does the CMP contain clearly defined process for notifying the organisation's media and public relations department/representatives?

Roles, Accountability, Responsibility and Authority.

- Is the role of the organisation's executive/senior management during a crisis clearly defined, agreed and documented?
- Has a senior manager (executive) been appointed as accountable for crisis management within the organisation?
- Does the CMP clearly define the organisation's crisis management roles, accountability(ies), responsibility(ies) and authority(ies)?
- Are all key staff fully aware of their Crisis Management roles, accountabilities, responsibilities and authority?

- Does the CMP contain details of any reservations concerning role accountability, responsibility or authority in its operation?
- Does the CMP contain details of any exclusions concerning role accountability, responsibility or authority in its operation?
- Does the CMP contain clearly defined instructions, advice, guidance and process concerning the authorisation of financial expenditure during a crisis?
- Has each CMP role been assigned to a principal individual
- Has each CMP role been assigned to an alternate individual should the principal be incapacitated or otherwise unavailable during a crisis?
- Has each CMP role been allocated to an appropriate level of authority to carry out the role accountabilities and/or responsibilities?
- Are all managers aware of their responsibilities to ensure compliance with the legal, regulatory and policy requirements for crisis management?

Key Supporting Information.

- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning key supporting information?

People Issues.

- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning casualties and fatalities?
- Does the CMP contain either mandatory instructions, advice, process, procedure, guidelines or service concerning confidential staff counselling?
- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning staff welfare e.g personal belongings, travel and relocation issues?
- Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning staff and public announcements?
- Have the organisation's Human Resources Department been consulted in the development of the organisation's strategy(ies) and plan(s)?
- Have Trade Unions and Staff Associations been consulted in the development of the organisation's crisis management strategy(ies) and plan(s)?

Communication.

- Does the CMP contain mandatory instructions, advice, process, procedure or guidelines concerning internal and external communications?

- Does the CMP have a clearly defined, up-to-date communication cascade and/or process (e.g. 0800 free phone) to ensure staff and all other stakeholders are kept informed?
- Does the CMP provide a clearly defined process for notifying staff and other stakeholders of telephone/fax/contact numbers?
- Does the CMP provide a clearly defined response to the failure of voice and/or data communication systems?
- Does the CMP provide approved preformatted messages?
- Are staff and managers provided with a pocket-size crisis management aide memoire?
- Are all staff and managers made fully aware of the significance of 'Legal Privilege' in all communications concerning a crisis?
- Does the CMP clearly identify relevant stakeholder groups and establish essential communication plans with them?
- Does the CMP provide clear information and a process for notifying the organisation's crisis management team(s) and maintaining lines of communication the its members?

Documentation/Forms/Checklists.

- Does the Crisis Management Plan (CMP) have an up-to-date task list(s) that clearly identifies both mandatory and discretionary tasks together with the roles accountable/responsible for their completion with an allocated timeframe?
- Does the CMP provide an auditable process for tracking and recording the completion of the CMP task list(s) after the plan has been invoked?
- Does the CMP provide an auditable process for tracking and recording the completion of additional/further ongoing tasks in addition to those contained within the CMP task list?
- Does the CMP provide up-to-date (internal and external) contact schedules/lists (e.g. key and alternate staff, suppliers, stakeholders)?
- Does the CMP provide a crisis management and decision log template?
- Does the CMP provide an impact assessment profile template?
- Does the CMP provide a telephone message form/log?
- Does the CMP provide a Business Relocation Recovery Profile?
- Does the CMP provide a list of the contents of the crisis management battlebox?

External Bodies and Organisations.

- Has an individual been clearly identified and appointed to the role of Emergency Services Liaison Officer within the CMP?
- Does the CMP provide clearly defined and documented co-ordination procedures for local authorities?
- Does the CMP provide clearly defined and documented co-ordination procedures for other relevant public authorities?
- Does the CMP provide clearly defined and documented co-ordination procedures for the utility services?

Media and Public Relations.

- Does the Crisis Management Plan (CMP) contain a clearly defined media and public relations strategy and plan?
- Does the CMP clearly identify and unambiguously describe stakeholders and interest groups?
- Does the CMP provide clearly defined and 'approved' generic media statements?
- Does the CMP clearly identify external liaison points/roles e.g. organisations, agencies and individuals?
- Does the CMP clearly identify individuals who have been trained to deal with the media?

Further Reading.

- Augustine, N.R, (1995) 'Managing the crisis you tried to prevent', Harvard Business Review, Vol.73, No.3, pp.147-158.
- Bland, M. (2002) 'Communicating out of a crisis', Globalcontinuity.com, pp.1-7.
- Charters, I. (2000) 'The reality of worst case scenarios', Continuity, Vol.4, No.4, pp.7-8.
- Elliott, D., Swartz, E., and Herbane, B. (1999) 'Just waiting for the next big bang: Business Continuity in the UK financial sector', Journal of Applied Management Studies, Vol.8, No.1, pp.43-60.
- 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 Reserve Bank, (2002) 'Implications of 9/11 for the financial services sector', Bank of International Settlement Review, pp.1-5.
- Ferguson, R.W. (2002) 'A supervisory perspective on disaster recovery and business continuity', Bank of International Settlement Review, pp.1-4.

- Fink, S. (1986) 'Crisis Management: Planning for the inevitable', Amacom, New York. ISBN 0-8144-5859-9.
- Flin, R. and Slaven, G. (1996) 'Personality and emergency command ability', Disaster Prevention and Management', Vol.5, No.1, pp.40-46.
- Gillions, P. (1988) 'Crises: The communications imperative', Disaster Management, Vol.1, No.2, pp.42-46.
- Heath, R. (1998) 'Standard 9: Public relations and crisis communication', Survive, Vol.2, No.2, pp.10-11.
- Home Office. (1992) 'Principles of Command and Control', HMSO, London.
- Home Office. (1996) 'How resilient is your business to disaster', HMSO, London.
- Home Office. (1999) 'Bombs: Protecting people and property', (4th Ed.) HMSO, London.
- Home Office. (2001) 'Business as usual: Maximising business resilience to terrorist bombing', HMSO, London.
- Honour, D. (2001) 'Heeding the lessons of 9/11', International Journal of Business Continuity Management, Vol.2, No.1, pp.13-17.
- McLean, R. (2001) 'From incident to disaster: Managing the escalation process', Continuity, Vol.5, No.3, pp.6-9.
- Mitroff, I.I. and Pearson, C.M. (1993) 'Crisis Management: A diagnostic guide for improving your organisations crisis preparedness', Jossey-Bass, San Francisco. ISBN 1-55542-563-1.
- Moore, T. (1994) 'Planning and training for a major disaster', Intersec, Vol.4, No.10, pp.329-331.
- Moore, T. (1997) 'Leadership in a major crisis', Intersec, Vol.7, No.5, pp.158-160.
- O'Reilly, S. (2000) 'Command and Control: The foundation of successful business continuity management', Insight, Vol.3, Issue.1, pp.10 -11.
- Payne, C.F. (1994) 'Handling the Press', Disaster Prevention and Management, Vol.3, No.1, pp.24-32.
- Power, P. (1999) 'Business Continuity Management: Preventing chaos in a disaster', Department of Trade and Industry, London.
- Power, P. (2001) 'Handling a Crisis: Perception or reality', Continuity, Vol.5, No.3, pp.4-5.
- Power, P. (2002) 'Crisis management teams: Who needs them?', Globalcontinuity.com, pp.1-5.

- Smith, D. (1990) 'Beyond contingency planning: Towards a model of crisis management', *Industrial Crisis Quarterly*, Vol.4, No.4, pp.263-275.
- Smith, D.J. (2001) 'A recipe for chaos', *Risk Management*, Vol.6, No.1, pp.9-14.
- Watson, W. 1992, 'Corporate communication in a crisis: Some vital questions', *Disaster Management*, Vol.4, No.2, pp.109-111.

Video.

Home Office (1995) 'Strategic: The Principles of Command and Control', Hawkshead Limited, London.

British Broadcasting Corporation (2002) 'Disaster 1; Spiral To Disaster', BBC Worldwide Limited, London.

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

North Yorkshire Police (1995) 'The Duneswick Aircrash: A Small Major Disaster', North Yorkshire Police, Northallerton, Yorkshire.

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

Cases Studies.

Aftermath of Multiple Murder in 1995 by Street, J. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.208-213. ISBN 0-33-72097-0

Bishopgate Bomb in 1993 in Hiles, A. and Barnes, P. (1999) 'The definitive handbook of Business Continuity Management', Wiley and Sons Ltd, Chichester, pp.332-334. ISBN 0-471-98622-4

'Cot Death' Poisonings in 1994 by Thomas, F. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.214-222. ISBN 0-33-72097-0

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.

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

Johnson and Johnson (Tylenol) in Fink, S. (1986) 'Crisis management - planning for the inevitable', Amacom, New York, pp.203-218. ISBN 0-8144-5859-9

Knight, R. F. and Pretty, D. J. (2000) 'The impact of catastrophes on shareholder value', Oxford Executive Research Briefings, Templeton College, Oxford.

Manchester Bombing in 1996 in HMSO (1999) ' Business As Usual - Maximising business resilience to terrorist bombings' pp.6-10.

Mercantile Fire in 1991 in Hiles, A. and Barnes, P. (1999) 'The definitive handbook of Business Continuity Management', Wiley and Sons Ltd, Chichester, pp.317-320. ISBN 0-471-98622-4

Odwalla Apple Juice in 1996 by Harrington, M.J. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.193-199. ISBN 0-33-72097-0

Pepsi Syringes in 1993 by Doeg, C. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.200-207. ISBN 0-33-72097-0

Procter and Gamble (Reply Tampon) in Fink, S. (1986) 'Crisis management - planning for the inevitable', Amacom, New York, pp.190-202. ISBN 0-8144-5859-9

Stena Challenger Grounding in 1995 by Simms, J. in Bland, M. (1998) 'Communicating out of a crisis' Macmillan Press Ltd, London, pp.181-192. ISBN 0-33-72097-0

Union Carbide (Bhopal) in Fink, S. (1986) 'Crisis management - planning for the inevitable', Amacom, New York, 196-189. ISBN 0-8144-5859-9.