BUSINESS CONTINUITY INSTITUTE

GOOD PRACTICE GUIDELINES 2007

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

CHAPTER 4

ABOUT THE GUIDE

Introduction

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

This new guide to implementation of Business Continuity Management (GPG07) has been prepared to support the launch of BS 25999-1 A Code of Practice for Business Continuity Management by the British Standards Institution. It can be viewed as implementation guide to BS25999 and as a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner.

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

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

Format of Guide

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

Chapter 1 consists of the introductory information plus **BCM Programme Management**.

Chapter 2 is **Understanding The Organisation**

Chapter 3 is **Determining BCM Strategy**

Chapter 4 is **DEVELOPING AND IMPLEMENTING BCM RESPONSE**

Chapter 5 is **Exercising, Maintaining & Reviewing BCM arrangements**

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

At the end of each chapter there is a summary of key learning outcomes that will support future use of the BCI Benchmarking tool, BCI E-Learning and BCI Entrance Examinations.

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

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

About Chapter 4 – Developing & Implementing a BCM Response

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

Determining and Implementing a BCM response is key to success or failure of a BCM programme. It covers the development of appropriate detailed action plans to ensure continuity of activities and effective incident management.

Chapter 4 – Developing & Implementing a BCM Response

CONTENTS.

GUIDELINES STAGE 4

DEVELOPING & IMPLEMENTING A BCM RESPONSE

COMPONENTS

1. INCIDENT RESPONSE STRUCTURE
2. INCIDENT MANAGEMENT PLAN
3. BUSINESS CONTINUITY PLAN
4. ACTIVITY RESPONSE PLANS

DEVELOPING & IMPLEMENTING A BCM RESPONSE

Reference: BS 2999-1 Section 8

General Principles

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

The key requirements for an effective response are:

- A clear procedure for escalation and control of an incident
- Communication with stakeholders
- Plans to resume interrupted activities

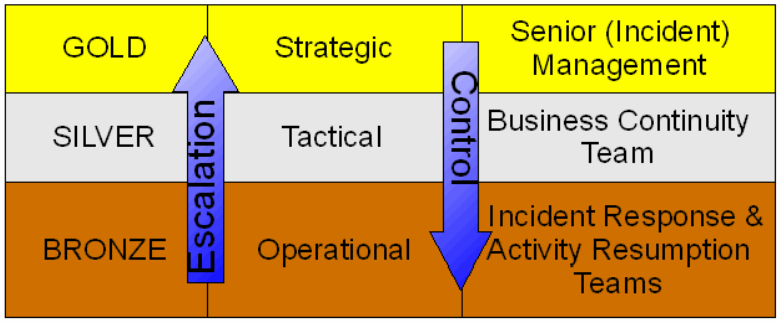
These outcomes can be achieved by various means and only one possible structure is described here. Whatever structure is adopted it is important that the chosen strategy fits with the culture of the organisation.

The actions outlined in plans are not intended to cover every eventually as, by their nature, all incidents are different. Any predefined procedures may need to be adapted with flexibility and initiative by those responsible for implementing the plan to the specific event that has occurred and the opportunities it may have opened up.

INCIDENT RESPONSE STRUCTURE

1. Introduction

One model of incident response, borrowed from the UK Emergency Services, shows three tiers of incident response often referred to as Gold, Silver and Bronze. When applied to an organisation's response structure the responsibilities are as follows.



Strategic Level - Incident Management Plan (IMP)

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

The Incident Management Plan is sometimes called a 'Crisis Management Plan'; however reporting in the media that you have invoked your 'Crisis Management Team' may lead people to think you feel you have a Crisis. The term 'Incident' has less negative connotations so is preferred in this document.

Tactical Level: Business Continuity Plan (BCP)

The BCP addresses business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed. They are based upon the agreed Business Continuity Strategies and provide procedures and processes for both the business continuity and resource recovery teams. In particular the plans allocate roles and their accountability, responsibility and authority. The plans must also detail the interfaces and the principles for dealing with a number of external players in the response such as recovery services suppliers and emergency services.

If the event falls outside the scope of the assumptions on which the Business Continuity Plan was based then the situation should be escalated to those responsible for implementing the Incident Management Plan (IMP).

Operational Level: Activity Resumption Plans

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

Timeline

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

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

Scalability

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

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

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

INCIDENT MANAGEMENT PLAN

Reference: BS 2999-1 Section 8.3-5

1. Introduction

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

2. Precursors

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

3. Purpose

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

4. Concepts and Assumptions

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

Some incidents will require an IMT response that do not result from disruption to activities for example those involving threats to reputation alone - and may therefore not involve a Business Continuity response. However, where a BC response is required there is almost always a need to involve the IMT if only to make them aware of the situation in case it escalates.

5. Process

The key steps in developing an Incident Management Plan include:

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

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

6. Methods and Techniques.

Building the Incident Management Plan

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

- Stakeholder analysis
- Scenario planning
- Checklist (s)
- Workshops
- IMP Templates for distribution to assist implementation of standard procedures in an international organisation with several IM teams

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

IMP Contents

As, by their nature, all crises are different the Incident Management Plan is a set of components and resources that may be useful to the team tasked with activating the plan. The contents will also depend on the nature and complexity of the organisation.

The Incident Management Plan should be modular in design so that single sections can be supplied to individuals and/or teams on a need-to-know basis. It is suggested that the different sections are printed on different coloured paper to provide ease of use at the time of a crisis.

Document owner and maintainer

The plan should have a nominated owner and procedure for maintenance.

Roles and Responsibilities

The roles of the team and specific individuals should be documented.

Deputies should be identified for each role.

Responsibilities for the team or nominated individuals may include:

- Managing communications (see section below)
- Ensuring IMT and BCT are properly staffed and making appointments if necessary
- Liaising with the Business Continuity Team to agree resumption timetable
- Approving significant expenditure
- Monitoring the overall progress of recovery and personnel performance
- Identifying and maximising opportunities or advantages arising from the incident
- Looking at the strategic impact of the incident on the organisation - which may require significant changes in direction or open up new opportunities
- Maintaining a decision log throughout the incident.

Invocation / mobilisation instructions

The circumstances in which the team will be activated should be documented, and the persons able to initiate the call-out decided. However, due to the nature of incidents, this should allow some flexibility and encourage action where this is doubt since it is easier to stand down an activated team than activate them after the incident has developed out of control.

The means by which the team will be activated should be documented so that decisions can be made in the shortest possible time.

The team should agree, in advance, a number of possible meeting locations favouring those with the required resources (see below). On invocation the first notified should identify the most suitable meeting place and a fallback, based on the current information.

Action plans

The plan should contain initial prompts for action - such as stakeholder list. The Business Impact Analysis may contain useful pointers to potential impacts that will need to be managed

Meeting room

At least two locations should be predefined to act as an incident management centre (control room). One is likely to be on-site where the senior management team are based but the other should be designated off-site.

The off-site location does not have to be owned by the organisation. A 24-hour hotel with a willing manager should be able to provide all the facilities required for most organisations.

Consideration should be given to how the space is best utilised for the needs of:

- communication - incoming and outgoing
- recording events, actions and issues
- monitoring broadcasting.
- controlled entry

Resources

The following resources should be considered:

- Whiteboard/flip charts (and pens that work)
- A number of telephones, including at least one with an ex-directory outgoing line and phone recording facility
- Hotline/helpline facility
- Mobile communicators, cell phones, fax, e-Mail and Internet
- TV and radio monitoring equipment
- TV/radio 'studio' facilities - to rehearse interviews
- ISDN line + camera for transmitting interviews straight to broadcast station and videoconferencing
- Stationery
- A means of logging all actions.
- Refreshments and nearby or on-site sleeping facilities
- A separate and nearby venue for hosting the press.

Hardware and information can be kept off-site at the alternative location in a locked trunk

(often called a 'battle-box').

People Activities

Organisations have a responsibility to safeguard the welfare of their employees, contractors, visitors and customers (which may be legally enforced). All BCM strategies should take into account welfare issues during an incident and the recovery phase. Staff are more likely to cooperate willingly with the extra demands if their welfare needs are met.

Issues to consider in planning include:

- Special needs of individuals during evacuations or stay-in periods including:
  - pregnancy
  - disabilities
  - family responsibilities

During an incident one or more individuals should assume responsibility for:

- Site evacuation
- Accounting for staff, contractors and visitors
- Communicating with staff and others on the site
- Contact with emergency contact or next of kin - local regulations may require that this should only be done in consultation with the emergency services
- Translation services
- Transport assistance
- Setting up a staff help line

Subsequently there may additional needs including:

- Temporary accommodation
- Counselling and rehabilitation services - this could be provided as part of an employee health package
- Welfare needs at alternative locations:
  - Special needs
  - Refreshments
  - Personal safety and security
  - Transport and accessibility

- Appropriate training on replacement equipment

Emergency services liaison

Staff with an appropriate level of experience and authority should be appointed to liaise with the emergency services at the arrival on site and subsequently as required.

The emergency services should be given information on the location of any casualties and the status of the situation and any known hazards they may encounter.

Whilst on the site, the emergency services instructions take precedence over those given by the organisation's own staff.

On departure from the site, the organisation will resume responsibility for its own site security.

Incident Communications Plan

The Incident Communications Plan should address how the organisation will manage communication with all stakeholders including:

- Staff, relatives, friends and emergency contacts
- Customers and suppliers
- Shareholders or owners
- (If part of a Group or larger organisation) liaising with other members of the group or head office
- Informing and liaising with regulatory authorities (following consultation with the organisation's legal and compliance functions)
- Dealing with issues relating to serious injuries or fatalities (in consultation with the Emergency Services and in accordance with local regulations and customs)
- Media - local and national newspapers, radio, TV, internet and other media

Consider in advance:

- What crises could hit us? (A Risk Assessment may be appropriate)
- Who are the Audiences?
- How do we communicate with them?
- What are the Messages?
- Who will form the Incident Team?
- What are the Resources and Facilities?
- Are the Incident team and spokespeople Trained?

- Does it Work?
- What Incident Manual do we need?
- Have we built lines of communication with our audiences?

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

If faced with a crisis consider:

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

7. Outcomes and Deliverables

The outcomes of the Incident Management Planning process include:

- A Incident Management Plan that can support the role of the organisation's Incident Management Team during a crisis event
- A Incident Communications Plan that can manage the media and stakeholder communication during a crisis
- Demonstration of preparation for effective Incident management to the media, markets, customers, stakeholders and regulators
- Compliance with statutory and regulatory requirements

8. Review

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

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

BUSINESS CONTINUITY PLAN

Reference: BS 2999-1 Section 8.3 & 8.6-7

1. Introduction

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

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

2. Precursors

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

3. Purpose

The purpose of a Business Continuity Plan(s) is to provide a documented framework and process to enable the organisations to resume all of its business processes within their RTO. A Business Continuity Plan on its own does not demonstrate a BCM competence or capability; but the presence of a current plan that has been produced by the organisation does suggest an effective capability

4. Concepts and Assumptions

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

The BC Plan will always contain (and should document) assumptions about the maximum scale of the incident (in terms of extent, duration or staff impact). If these are exceeded then this should be escalated to the Incident Management Team to resolve since the solution will, almost inevitably, involve a strategic decision.

5. Process

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

- Appoint an owner for the BC Plan (or each plan for multiple sites)

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

6. Methods and Techniques

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

A variety of software products are available to assist in building and maintaining a Business Continuity Plan however it is not essential. Using normal office software (Word processor and spreadsheet) may suffice and is more inclusive of all staff since its use does not require special training. Customised software can however provide significant benefits in the areas of plan maintenance and referential integrity.

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

The plan should contain:

Document owner and maintainer

The person or group nominated to ensure the plan remains up to date and effective.

Roles and Responsibilities

The roles of the team and specific individuals should be documented.

Deputies should be identified for each role.

Responsibilities of the team or specific individuals may include:

- Liaising with the Emergency Services
- Receiving or seeking information from response teams
- Reporting information to the Incident Management Team
- Mobilising third-party suppliers of salvage and recovery services
- Allocating available resources to recovery teams

Invocation / mobilisation instructions

The circumstances in which the team will be activated should be documented, and the persons able to initiate the call-out decided. However, due to the nature of incidents, this should allow some flexibility and encourage action where this is doubt since it is easier to stand down an activated team than activate them after the incident has developed out of control.

The means by which the team will be activated should be documented so that decisions can be made in the shortest possible time.

The team should agree, in advance, a number of possible meeting locations favouring those with the required resources (see below). On invocation the first notified should identify the most suitable meeting place and a fallback, based on the current information.

Action plans / task list

Detailed procedures for the team to:

- Respond to invocation
- How decisions are to be taken
- Mobilise resources
- Initiate activity recovery
- Receive information from other teams
- Report status to Incident Management team

Resource requirements

Lists of the available resources:

- Personnel
- Facilities and supplies
- Technology, communications and data
- Security
- Transportation and logistics
- Welfare requirements
- Emergency cash and payments

Contact information to access those resources

Resource Requirements for resumption of each Activity

Vital information

Customer information

Contact details

Legal documents - such as contracts and insurance policies

Service level agreements

Forms and annexes

Checklists to assist recovery

7. Outcomes and Deliverables

The deliverables of the Business Continuity Management planning process include:

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

8. Review

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

- A significant change in the technology and/or telecommunications
- There is a major business process change

- A significant change in staff
- A change in the supplier of BCM solutions

ACTIVITY RESPONSE PLANS

1. Introduction

A Business Continuity Plan will rapidly become unwieldy if all recovery procedures are included in a single document. When this becomes the case (in medium-sized or large organisations) the response and recovery plans of each activity should be taken out of the BCP and made a separate document that becomes the responsibility of the Activity to which it relates.

The Activity (Operational level) Response Plans cover the response by each department or business unit to the incident. Examples of Operational Response plans are:

- Procedures to assist an incident response team usually lead by a Facilities department who deal with the specific incident and its physical impact (if any)
- A Human Resources response to welfare issues in an incident
- A business department plan to resume its functions within a predefined timescale
- An IT department's logistical response to the loss and subsequent resumption of IT services to the business

The complexity and urgency of the business processes may determine whether one operational plans covers a single activity or a department covering several activities.

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

2. Precursors

Because of the many links between the BC Plan and those of the Operational Response, the BC Plan should be written, at least in outline, before these operational plans are finalised.

3. Purpose

The purpose of the Operational Response Plan is to structure the response of each department to an interruption within the overall Business Continuity Plan.

4. Concepts and Assumptions

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

5. Process

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

- Appoint a person to be responsible for development of the plans overall and a

representative within each operational unit to develop their plan

- Define the objective and scope of the plans
- Develop a planning process and timetabled programme. Where possible, begin with the plans for the most urgent business activities
- Determine the overall BCM strategies on which the plan is based.
- Decide the structure, format, components and content of the plans
- Develop an outline or template plan to encourage standardisation of documentation but allow individual variations where this is appropriate
- Ensure that BUs nominate individuals to fulfil roles within their plans
- Manage and mentor the development of plans within the BUs
- Circulate the draft of the plan for consultation, review and challenge within and, where necessary outside, the department
- Gather feedback from consultation
- Amend plan as appropriate
- Validate the plan through a unit test
- Consolidate the BU plans and review for consistency
- Document connections with the BC Plan and between Unit plans
- Conduct a resource requirements analysis across all plans to define resource requirements for support functions

6. Methods and Techniques

The methods, tools and techniques to develop a Operational Response Plan include:

- Interviews (structured and unstructured)
- A Business Impact Analysis and Resource Requirements analysis for this activity (to refine the findings of the higher level BIA)
- Checklists and templates
- Workshops

Specific Operational Response plans may include the following:

Facilities (Incident Response Team)

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

Human Resources

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

Business Unit Resumption

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

- Work in Progress issues
- Staff numbers
- Consumables required

7. Outcomes and Deliverables

The outcomes of the Operational Response Plan include:

- A documented Operational Response Plan for each business activity or department
- Criteria for BU to escalate issue to BCT
- Clearly defined BCM roles within the department

8. Review

Operational Response plans should be reviewed if there is a major change in the business process or technology within that area.

KEY BCM INDICATORS

The following are key elements of what would be expected from a mature BCM organisation.

1. The organisation owns one or more Incident Management Plan and Business Continuity Plan, enabling it to manage any potential continuity incident or crisis in any part of the business regardless of cause

2. The organisation operates one or more incident and recovery teams who are responsible for managing all potential continuity-threatening incidents

3. Each team includes senior accountable individuals with the authority and knowledge to respond effectively to any incident

4. Each team member has at least one similarly empowered and trained deputy or successor

5. Each team is mandated and provisioned so it can be always mobilised in time to deliver an appropriate response

6. Each team has to hand all the necessary tools and information that it requires to manage an incident

7. All team members have been appropriately trained to operate under crisis or similar conditions

8. Each plan defines an escalation and invocation process that allows for its rapid or immediate activation

9. Each contains unambiguous invocation instructions for all types of incident and conditions

10. Each contains clear invocation criteria and guidelines

11. Each plan clearly identifies those who have authority to invoke it

12. Each contains tasks and checklists to contain the immediate consequences of a business disruption

13. Each contains a clear and unambiguous statement of its purpose and scope

14. Each plan explains emergency communications and warning protocols and mechanisms

15. Each requires next-of-kin and emergency contact information for all personnel are kept up-to-date and available for prompt use

16. Each identifies the person (s) who will discharge responsibility for welfare issues following an incident

17. Each plan contains specific guidance ensuring that human welfare issues are addressed as a priority and effectively managed following any incident

18. Each plan defines and communicates the roles, responsibilities and authorities of all participants

19. Each plan contains and establishes a clear framework for the acceptable control of any incident

20. Each plan clearly describes how to select, adapt and implement strategies to optimise recovery from the incident

21. Each plan contains clear statements of prioritisation, reflecting seasonal, periodic and intra-day variations

22. Each plan clearly identifies the recovery levels that must be achieved over time (recovery time objectives)

23. Each plan clearly describes means for co-ordinating all teams and entities involved in the recovery

24. Each plan contains tasks, procedures and checklists that initiate and acceptably deliver the strategies

25. Each plan contains an up-to-date inventory of the resources required over time to acceptably deliver the strategies

26. Each plan contains logs or forms for the recording of information about the incident

27. Each plan contains tasks and checklists for restoring normal operations after any incident

28. Each plan contains tasks that provide effective situation analysis and damage assessment

29. Each plan contains tasks that assure continuity of each material outsourcing agreement

30. Each plan provides reliable indication of the time to complete each plan step under disruption conditions

31. Each plan includes or references up-to-date contact and mobilisation details for all key stakeholders.

32. The organisation's plans specifically provide for timely managed communication during, pre- and post-incident with all key stakeholders

33. Appropriate governance provisions are specifically assured by the incident plans

34. Each plan identifies staff with appropriate levels of authority to liaise with the emergency services

35. Each plan provides the basis for an effective crisis information management system

36. Each plan specifies the means and frequency for providing information e.g. press releases, email, websites

37. Each plan provides a strategy and framework for communicating with the media

38. Each plan identifies trained and competent spokespeople who are authorised to release

information to the media

39. Each plan identifies a preferred venue for liaison with the media or other stakeholder groups

40. Each plan documents how to monitor the media response

41. Plans contains a template statement to the media

42. Plans contains guidelines for public awareness-raising via the media

43. Each plan identifies a primary location from where the incident will be managed by preference (incident management location)

44. Each plan identifies an alternative location, in case access to the primary incident management location is denied

45. Each incident management location provides access to the resources required to promptly expedite the incident plan

46. Each incident management location provides for effective primary and alternative means of communication

47. Each incident management location provides facilities for accessing and sharing information, including monitoring of news media

48. Each plan is concise and easily assimilated by all of its potential users

49. Each plan is practical and action-oriented and excludes all information that will not be required during an incident

50. Each plan is readily accessible by all of its potential users

51. Each plan is complete in that it addresses any disruption from the point of discovery to the resumption of normal business operations

52. Each plan is complete in that it documents all the components required to reliably implement each of the strategies

53. Each plan identifies its responsible owner

54. Each plan has senior management support including a designated sponsor

55. Each plan identifies all those responsible for its regular review, maintenance and authorised release

56. Each plan is supported by an appropriate budget for its development and upkeep

57. Each plan complies with all relevant statutory and regulatory requirements

58. Each plan clearly describes its relationship with all other relevant plans or documents

59. Each plan and its associated documentation is up-to-date and reflects the organisation's current requirement

60. Each plan is subject to systematic version and distribution control

61. Each is formally signed off by senior management

Chapter 5 of the Good Practice Guidelines examines:

Exercising, Reviewing and Maintaining Plans