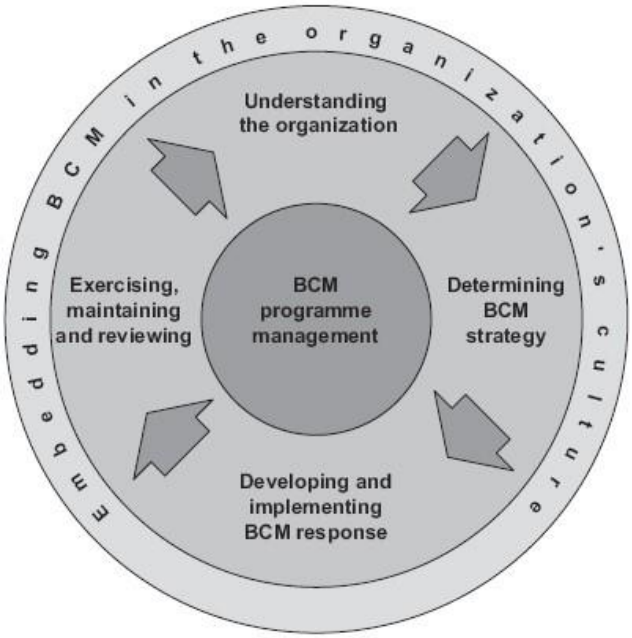
18 Business Continuity Management

Business Continuity is the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.

Business Continuity Management follows a cyclical process of analysis to understand threats and requirements, determination and implementation of contingency strategies, and the validation of planned response through testing and exercising.



BSI BS25999 Lifecycle

Before you start the BC programme, it is advisable to get buy-in from top management and key staff, define and win approval for a project budget, and set detailed timelines for the programme.

18.1.1 **Programme Management**

In order to implement and maintain an effective business continuity programme, it is imperative that the TOC establishes a Business Continuity Management System (BCMS). Whilst this should be under the coordination of a designated business continuity manager, it is vital that the BC programme is sponsored at the highest level in the organisation, and the following documentation should be signed off by top management. The BCMS should contain the following elements:

18.1.2 **Definition of Scope**

- Services and locations covered by the business continuity programme
- Organisational objectives and obligations
- Acceptable level of Risk
- Planning assumptions
- Statutory, regulatory and contractual duties
- Interests of key stakeholders

18.1.3 **Business Continuity Policy**

- Strategic prioritisation of assets and services
- What the organisation will undertake to implement and maintain the BCMS
- Roles and responsibilities
- Statement of endorsement by top management sponsor
- BC programme communication and awareness programme

18.1.4 **Policies for Establishing, Maintaining and Reviewing Plans**

- Provision of Resources
- Competency of BCM personnel
- Business Impact Analysis
- Risk Assessment
- Incident Response Structure
- BCM Exercising, testing and training
- Maintenance and Review of BCM arrangements
- Internal Audit
- Management Review
- Preventative and Corrective Actions

18.1.5 **Understanding the Organisation**

In order to implement appropriate contingency strategies, it is necessary to take a structured approach to understanding critical business needs. The two main tools applied in the business continuity programme are the risk analysis and Business Impact Analysis (BIA) processes. The outcome of the risk analysis and BIA is to gain a full understanding of the threats and resource dependencies for the activities that make up the key services of the TOC.

18.1.6 **The Risk Analysis Process**

In most organisations, a formal risk analysis process is already undertaken, and it is vital that operational risk outcomes from this process are understood in the context of the business continuity programme. The Risk Analysis process should include:

- Gathering of data on threats and previous incidents
- Scoring of threats against likelihood and impact
- Assignment of a plan for individual risks (Treat, Tolerate, Transfer, Terminate)
- Assigning responsibility/deadlines for treatment plans
- Regular Formal review of Risk Analysis by defined committee (as defined in the BCMS

18.1.7 **The Business Impact Analysis**

The BIA is the single most important, and generally time consuming, process in the business continuity programme. The purpose of the BIA is to define the criticality of the activities that make up the TOC's services, and to identify the resources on which this activity depends (NB. The data from this process

is most valuable at “activity” rather than “service” level). The data gathering process that should be followed is:

- Identify services and departments defined in BCMS scope
- Define the impact of activity disruption, and therefore business’ acceptable period of activity disruption
- Define all resource dependencies (location, staff, IT support, technology, etc)
- Define the minimum resources required to re-commence activity over time
- Define the recovery times for each resource on which the activity depends; ensure that the recovery time is less than the tolerable period of disruption.

18.1.8 **The Plan**

Once the BIA and risk analysis have been completed, strategies for incident response can be developed. Data from the analyses will indicate which activities are most critical to the organisation, and what the likely threats to their continuation are. The response strategy, as detailed in the plan, should be devised in line with this intelligence.

18.1.9 **The Incident Response Structure**

Each team within the incident response structure should have a plan. Typically, organisations will follow a three tier Gold (strategic), Silver (tactical) and Bronze (departmental) command structure. All teams should be supported by a trained executive support team.

The incident response structure should identify process to:

- Confirm nature and extent of an incident
- Trigger an appropriate BC response
- Have plans, processes and procedures for the activation, operation, coordination and communication of the incident response
- Have resources available to support plans, processes and procedures to manage an incident
- Communicate with stakeholders

The roles of these teams are:

- Overall Incident Management
- Set Strategic aims & objectives

Gold

(Strategic)

- Media
- Communications & Liaison (Internal/Key Stakeholders)
- Resolve Silver/Tactical level resource issues
- Plan for Recovery

- Assess risks
- Allocate and Manage resources to achieve Strategic

Silver

aims/objectives

(Tactical) Plan and Coordinate Operational activity

- Communications & Liaison (Internal/Key Stakeholders)
- Resolve/Escalate Bronze/Operational level resource

Bronze (Operational)

- Undertake tasks and activities as directed by Silver
- Escalate resource constraints to Silver
- Communications & Liaison (largely internal)

18.1.10 **The Plan Itself**

The plan itself should be a useable document, available to the response teams at the point of need. All responding staff should be familiar with the plan. All teams identified in the incident response structure should have ownership of their own plan. Each plan should:

- Have a defined purpose and scope
- Be accessible to and understood by those who will use them
- Be owned by a named person who is responsible for their review, update and approval
- Be aligned with relevant contingency arrangements external to the organisation • Identified lines of comms

18.1.11 **Key tasks and reference information**

- Defined roles and responsibilities for people and teams having authority during and following an incident
- Guidelines and criteria regarding which individuals have the authority to invoke each plan and under what circumstances
- Invocation method
- Meeting locations and alternates, up to date contact lists and mobilisation details for any relevant agencies, organisations or resources
- Process for standing down
- Essential contact details for all key stakeholders
- Details to manage the immediate consequences of a business disruption including:
  - Welfare of individuals
  - Strategic & Operational options for responding to the disruption ○ Prevention of further loss or unavailability of critical activities
- Details for managing an incident including:
  - Provision for managing issues during an incident ○ Processes to enable continuity and recovery of critical activities

- How the organisation will communicate with staff, their relatives, stakeholders and emergency contacts

18.1.12 **Details of organisation's media response including:**

- The incident communications strategy
- Preferred interface with the media
- Guideline or template for drafting a statement
- Appropriate spokespeople
- Method for recording key information about the incident, actions taken and decisions made
- Details of actions and tasks to be performed
- Details of the resources required for BC/recovery at different points in time

18.2 Maintaining and Reviewing Plans

A plan can only be considered to be reliable once it has been exercised. It is also vital that the plan is maintained in line with the policies documented in the BC management system.

Procedures should be adopted that ensure a structured approach to exercising, corrective and preventative measures, management review and (internal) audit.

Exercising the plans, at departmental, tactical and strategic level is the most effective way of ensuring that key staff are familiar with the response strategy, and that the plans meet their aim. All plan holders should be exercised at least annually, according to a progressive exercise schedule. Exercises can be as simple as a desktop walkthrough of plans, through to complex simulations. It is recommended that the complexity of exercises develops with the confidence of the teams. The organisation should:

- Exercise to ensure BCM arrangements meet business requirements
- Develop Exercises consistent with the scope
- Have an Exercise programme approved by top management to ensure Exercises are held at regular intervals / after significant change
- Undertake a range of Exercises to validate the whole BC plan
- Plan Exercises to minimise the risk of the Exercise causing disruption
- Define aims and objectives of every Exercise
- Undertake a post Exercise review to assess achievement of Exercise aims and objectives
- Produce a written report of the Exercise – outcome, feedback and actions required

18.2.1 **Corrective and Preventative Measures**

The organisation should take action to guard against potential incidents and prevent their occurrence (or re-occurrence). Preventative and corrective actions taken shall be appropriate to the potential problems. The documented procedure should define requirements to:

- Identify potential issues and their causes
- Determine and implement actions needed
- Record results of actions taken

- Identify changed risks and ensure that attention is focussed on significant changed risks
- Ensure that all those who need to know are informed of the issue and actions • Prioritise actions in alignment with RA and BIA

18.2.2 **Management review**

Management should review the business continuity management system and programme at planned intervals and when significant changes occur. The review should include opportunities for improvement and the need for change in the BC management system. The results of the reviews should be clearly documented.

18.2.3 **Audit**

The audit processes for the Business Continuity programme should be consistent with the TOC's organisational audit procedure. It is however strongly recommended that any auditor undertaking a review of business continuity plans at the TOC has appropriate experience within the field of business continuity.

Any audit programme should be planned, established, implemented and maintained by the organisation taking into account the BIA, RA control and mitigation measures from the results of previous audits.

Audit procedure(s) shall be established, implemented and maintained that address:

- The responsibilities, competencies and requirements for planning and conducting audits, reporting results and retaining associated records
- The determination of audit criteria, scope, frequency and methods

18.2.4 **Conclusion**

However diligent the risk analysis process, however well managed the health and safety programme is, however well maintain stock is – incidents will always occur.

The ability of an organisation to respond to an incident is significantly improved by following a structured business continuity programme. The reputation of the organisation will be under close scrutiny in the aftermath of an incident – plans that meet the pre-determined continuity challenges of an organisation, carried out by trained teams are the best.