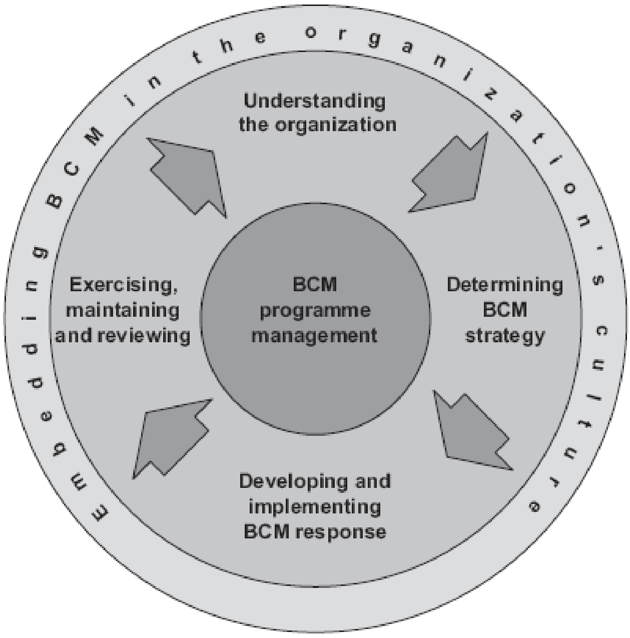
19. Business Continuity Management

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

19 Business Continuity Management

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

Business continuity management follows a cyclical process of analysis to understand threats and requirements, determine and implement contingency strategies and validate planned response through testing and exercising.


Embedding BCM in the organization's culture
Understanding the organization
Determining BCM strategy
Developing and implementing BCM response
Exercising, maintaining and reviewing
BCM programme management

BSI BS25999 life cycle

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

19.1.1 Programme management

In order to implement and maintain an effective business continuity programme, the TOC must establish a Business Continuity Management System (BCMS). Whilst this should be under the co-ordination 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:

19.1.2 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

19.1.3 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

19.1.4 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

19.1.5 Understanding the organisation

Implementing appropriate contingency strategies requires a structured approach to understanding critical business needs. The two main tools applied here are risk analysis and business impact analysis (BIA). These help to give a full understanding of the threats and resource dependencies for the activities that make up the key services of the TOC.

19.1.6 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. It should include:

- Gathering data on threats and previous incidents
- Scoring threats against likelihood and impact
- Assigning a plan for individual risks (treat, tolerate, transfer, terminate)
- Assigning responsibility/deadlines for treatment plans
- Regular formal review of risk analysis by a defined committee (as defined in the BCMS)

19.1.7 The business impact analysis

The BIA is the single most important, and generally time-consuming, process in the business continuity programme. Its purpose is to define the criticality of the activities that make up the TOC's services and identify the resources on which these activities depend (N.B.: the data from this process is most valuable at activity rather than service level). The data-gathering should:

- Identify services and departments defined in the BCMS scope
- Define the impact of activity disruption and therefore 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 recovery times for each resource on which the activities depend; ensure that the recovery time is less than the tolerable period of disruption

19.1.8 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 have trained executive support.

The incident response structure should identify processes to:

- Confirm the nature and extent of an incident
- Trigger an appropriate BC response
- Develop plans, processes and procedures for the activation, operation, co-ordination 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:

Gold (Strategic)

- Overall incident management
- Setting strategic aims & objectives
- Media
- Communications & liaison (internal/key stakeholders)
- Resolve Silver-/tactical-level resource issues
- Plan for recovery

Silver (Tactical)

- Assess risks
- Allocate and manage resources to achieve strategic aims/objectives
- Plan and co-ordinate operational activity
- Communications & liaison (internal/key stakeholders)
- Resolve/escalate Bronze/operational-level resource issues

Bronze (Operational)

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

19.1.9 The plan

The plan itself should be a useable document available to all response teams at the point of need. All responding staff should be familiar with it a and 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 all those who will use it
- Be owned by a named person who is responsible for its review, update and approval
- Be aligned with relevant contingency arrangements external to the organisation

- Identify lines of communication

19.1.10 **Key tasks and reference information**

- Defined roles and responsibilities for people and teams with authority during and following an incident
- Guidelines and criteria regarding which individuals have the authority to invoke each plan under what circumstances
- Invocation method
- Meeting locations and alternatives, 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 and 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

19.1.11 **Details of the organisation's media response**

- 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

19.2 Maintaining and reviewing plans

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

Procedures should 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 plans should be exercised at least annually according to a progressive exercise schedule. Exercises can be as simple as a desktop walk-through 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 they are held at regular intervals/after significant changes
- Undertake a range of exercises to validate the overall BC plan
- Plan exercises to minimise the risk of them causing disruption
- Define the aims and objectives of every exercise
- Undertake a post-exercise review to assess achievement of aims and objectives
- Produce a written report of the exercise – outcome, feedback and actions required

19.2.1 **Corrective and preventative measures**

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

- Identify potential issues and their causes
- Determine and implement the actions needed
- Record the results of actions taken
- Identify changed risks and focus attention on significant changed risks
- Ensure that all those who need to know are informed of the issue and actions
- Prioritise actions in alignment with the RA and BIA

19.2.2 **Management review**

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

19.2.3 **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) should address:

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

19.2.4 **Conclusion**

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

The ability of an organisation to respond to an incident is significantly improved by a structured business continuity programme. The reputation of the organisation will be under close scrutiny in the aftermath of an incident; plans must be well executed and meet the pre-determined continuity challenges of an organisation.