BRITISH STANDARD

# Business continuity management –

## Part 1: Code of practice

ICS 03.100.01

## Publishing and copyright information



ISBN 0 580 49601 5

The following BSI references relate to the work on this standard:
Committee reference BCM/1
Draft for comment 06/30139869 DC

## Publication history

First published November 2006

## Amendments issued since publication

| Amd. no. | Date | Text affected |
|---|---|---|

# Contents





**Summary of pages**

This document comprises a front cover, an inside front cover, pages i to iii, a blank page, pages 1 to 42, an inside back cover and a back cover.

# Foreword

## Publishing information

This British Standard was published by BSI and came into effect on 30 November 2006. It was prepared by Technical Committee BCM/1, *Business continuity management*. Organizations represented on this committee include:

Association of British Certification Bodies

Association of British Insurers

Association of Chief Police Officers

Association of Insurance Risk Managers

Business Continuity Institute

Cabinet Office

Chief Fire Officers' Association (CFOA)

Continuity Forum

Coventry University

Department of Trade and Industry

Emergency Planning Society

Federation of Small Businesses

Financial Services Authority

Independent International Organization for Certification

Institute of Directors

Institute of Emergency Management

Institute of Internal Auditors

Institute of Risk Management

Intellect

Metropolitan Police

Securities Industry Business Continuity Management Group (SIBCMG)

Society of Industrial Emergency Services Officers (SIESO)

Survive

This British Standard has been developed by practitioners throughout the business continuity community, drawing upon their academic, technical and practical experiences of business continuity management (BCM). It has been produced to provide a system based on good practice for business continuity management. It is intended to serve as a single reference point for most situations where business continuity management is practised, and to be used by large, medium and small organizations in industrial, commercial, public and voluntary sectors.

This document constitutes Part 1 of BS 25999. At the time of publication, Part 2 was in preparation which will specify requirements for business continuity management.

## Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

## Presentational conventions

The provisions of this Standard are recommendations, which are expressed in sentences in which the principal auxiliary verb is "should". Clause **3** does not contain any recommendations; rather, it gives useful background information on business continuity management (though the Standard is not intended as a beginner's guide to business continuity management).

The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility**,** e.g. a consequence of an action or an event.

*Supplementary commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.*

## Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

**Compliance with a British Standard cannot confer immunity from legal obligations.**

*This page deliberately left blank*

# 1 Scope and applicability

This British Standard establishes the process, principles and terminology of **business continuity management** (BCM). The purpose of this Standard is to provide a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in the organization's dealings with customers and other organizations. It also enables the organization to measure its BCM capability in a consistent and recognized manner.

This Standard provides a system based on BCM good practice.

This Standard is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization; from those with a single site to those with a global presence; from sole traders and small-to-medium enterprises (SMEs) to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation.

This Standard does not cover the activities of **emergency planning** inasmuch as that topic relates to **civil emergencies.**

*NOTE Ultimately, no matter how much effort or resource is invested in business continuity management, an organization could still be faced with an incident or combination of incidents it did not forsee.*

# 2 Terms and definitions

For the purposes of this part of BS 25999, the following definitions apply.

## 2.1 activity

process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services

*NOTE Examples of such processes include accounts, call centre, IT, manufacture, distribution.*

## 2.2 business continuity

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

## 2.3 business continuity management (BCM)

holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

*NOTE Business continuity management involves managing the recovery or continuation of business activities in the event of a business disruption, and management of the overall programme through training, exercises and reviews, to ensure the* ***business continuity plan(s)*** *stays current and up-to-date.*

### 2.4 business continuity management lifecycle

series of business continuity activities which collectively cover all aspects and phases of the **business continuity management programme**

*NOTE The business continuity management lifecycle is illustrated in Figure 1.*

### 2.5 business continuity management programme

ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review

### 2.6 business continuity plan (BCP)

documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level

### 2.7 business continuity strategy

approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption

### 2.8 business impact analysis

process of analysing business functions and the effect that a business disruption might have upon them

### 2.9 civil emergency

event or situation which threatens serious damage to human welfare in a place in the UK, the environment of a place in the UK, or the security of the UK or of a place in the UK [UK Civil Contingencies Act 2004 (1)]

### 2.10 consequence

outcome of an incident that will have an impact on an organization's objectives

*NOTE 1 There can be a range of consequences from one incident.*

*NOTE 2 A consequence can be certain or uncertain and can have positive or negative impact on objectives.*

### 2.11 cost-benefit analysis

financial technique that measures the cost of implementing a particular solution and compares this with the benefit delivered by that solution

*NOTE The benefit may be defined in financial, reputational, service delivery, regulatory or other terms appropriate to the organization.*

### 2.12 critical activities

those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives

### 2.13 disruption

event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives

### 2.14 emergency planning

development and maintenance of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency

### 2.15 exercise

activity in which the **business continuity plan(s)** is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect

*NOTE An exercise can involve invoking business continuity procedures, but is more likely to involve the simulation of a business continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.*

### 2.16 gain

positive **consequence**

### 2.17 impact

evaluated consequence of a particular outcome

### 2.18 incident

situation that might be, or could lead to, a business disruption, loss, emergency or crisis

### 2.19 incident management plan

clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process

### 2.20 invocation

act of declaring that an organization's business continuity plan needs to be put into effect in order to continue delivery of key products or services

## 2.21 likelihood

chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities

*NOTE 1 Likelihood can be expressed qualitatively or quantitatively.*

*NOTE 2 The word "probability" can be used instead of "likelihood" in some non-English languages that have no direct equivalent. Because "probability" is often interpreted more formally in English as a mathematical term, "likelihood" is used throughout this Standard with the intention that it is given the same broad interpretation as "probability".*

## 2.22 loss

negative **consequence**

## 2.23 maximum tolerable period of disruption

duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed

## 2.24 organization

group of people and facilities with an arrangement of responsibilities, authorities and relationships

*EXAMPLE Company, corporation, firm, enterprise, institution, charity, sole trader or association, or parts or combinations thereof.*

*NOTE 1 The arrangement is generally orderly.*

*NOTE 2 An organization can be public or private.*
*[BS EN ISO 9000:2005]*

## 2.25 products and services

beneficial outcomes provided by an organization to its customers, recipients and stakeholders, e.g. manufactured items, car insurance, regulatory compliance and community nursing

## 2.26 recovery time objective

target time set for:

- resumption of product or service delivery after an incident; or
- resumption of performance of an activity after an incident; or
- recovery of an IT system or application after an incident.

*NOTE The recovery time objective has to be less than the **maximum tolerable period of disruption**.*

## 2.27 resilience

ability of an **organization** to resist being affected by an incident

### 2.28 risk

something that might happen and its effect(s) on the achievement of objectives

*NOTE 1 The word "risk" is used colloquially in various ways, as a noun ("a risk" or, in the plural, "risks"), a verb (to risk [something], or to put at risk), or as an adjective ("risky"). Used as a noun the term "a risk" could relate to either a potential event, its causes, the chance (likelihood) of something happening, or the effects of such events. In risk management (see **6.5**) it is important to make a clear distinction between these various usages of the word "risk".*

*NOTE 2 Risk is defined relative to a particular objective; therefore, concern for several objectives implies the possibility of more than one measure of risk with respect to any source of risk.*

*NOTE 3 Risk is often quantified as an average effect by summing the combined effect of each possible consequence weighted by the associated likelihood of each consequence, to obtain an "expected value". However, probability distributions are needed to quantify perceptions about the range of possible consequences. Alternatively, summary statistics, such as standard deviation, may be used in addition to expected value.*

### 2.29 risk appetite

total amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time

### 2.30 risk assessment

overall process of risk identification, analysis and evaluation

### 2.31 risk management

structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk

### 2.32 stakeholders

those with a vested interest in an organization's achievements

*NOTE This is a wide-ranging term that includes, but is not limited to, internal and "outsourced" employees, customers, suppliers, partners, employees, distributors, investors, insurers, shareholders, owners, government and regulators.*

### 2.33 top management

person or group of people who direct and control an organization at the highest level [BS EN ISO 9000:2005]

*NOTE Top management, especially in a large multinational organization, might not be directly involved; however, top management accountability through the chain of command is manifest. In a small organization, top management might be the owner or sole proprietor.*

# 3 Overview of business continuity management (BCM)

## 3.1 What is BCM?

**Business continuity management (BCM)** is a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- proactively improves an organization's **resilience** against the disruption of its ability to achieve its key objectives;
- provides a rehearsed method of restoring an organization's ability to supply its key **products and services** to an agreed level within an agreed time after a disruption; and
- delivers a proven capability to manage a business disruption and protect the organization's reputation and brand.

While the individual processes of business continuity can change with an organization's size, structures and responsibilities, the basic principles remain exactly the same for voluntary, private or public sector organizations, regardless of their size, scope or complexity.

## 3.2 BCM and organizational strategy

All organizations, whether large or small, have aims and objectives, such as to grow, to provide services and to acquire other businesses. These aims and objectives are generally met via strategic plans to achieve an organization's short, medium and long term goals. BCM understanding at an organization's highest level will ensure that these aims and objectives are not compromised by unexpected disruptions.

The **consequences** of an incident vary and can be far-reaching. These consequences might involve loss of life, loss of assets or income, or the inability to deliver products and services on which the organization's strategy, reputation or even survival might depend.

BCM needs to recognize the strategic importance of known **stakeholders**. Furthermore, as the consequences of a disruption unfold, new stakeholders emerge and have a direct impact on the eventual extent of the damage. For example, issue groups may attempt to apply pressure on the organization facing a disruption.

All these issues are of strategic concern to the organization.

## 3.3 BCM – the relationship with risk management

BCM is complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks.

Risk management seeks to manage risk around the key products and services that an organization delivers. Product and service delivery can be disrupted by a wide variety of incidents, many of which are difficult to predict or analyse by cause.

By focusing on the impact of disruption, BCM identifies those products and services on which the organization depends for its survival, and can identify what is required for the organization to continue to meet its obligations. Through BCM, an organization can recognize what needs to be done before an incident occurs to protect its people, premises, technology, information, supply chain, stakeholders and reputation.

With that recognition, the organization can then take a realistic view on the responses that are likely to be needed as and when a disruption occurs, so that it can be confident that it will manage through any consequences without unacceptable delay in delivering its products or services.

An organization with appropriate BCM measures in place might be able to take advantage of opportunities which have a high risk.

## 3.4 Why an organization should undertake BCM

BCM forms an important element of good business management, service provision and entrepreneurial prudence.

Managers and owners have the responsibility to maintain the ability of the organization to function without disruption. Organizations constantly make commitments or have a duty to deliver products and services, i.e. they enter into contracts and otherwise raise expectations. All organizations have moral and social responsibilities, particularly where they provide an emergency response or a public or voluntary service. In some cases, organizations have statutory or regulatory duties to undertake BCM.

All business activity is subject to disruptions, such as technology failure, flooding, utility disruption and terrorism. BCM provides the capability to adequately react to operational disruptions while protecting welfare and safety.

BCM ought now to be regarded, not as a costly planning process, but as one that adds value to the organization.

## 3.5 The benefits of an effective BCM programme

The benefits of an effective BCM programme are that the organization:

- is able to proactively identify the impacts of an operational disruption;
- has in place an effective response to disruptions which minimizes the impact on the organization;
- maintains an ability to manage uninsurable risks;
- encourages cross-team working;
- is able to demonstrate a credible response through a process of exercising;
- could enhance its reputation; and
- might gain a competitive advantage, conferred by the demonstrated ability to maintain delivery.

## 3.6 The outcomes of an effective BCM programme

The outcomes of an effective BCM programme are that:

- key products and services are identified and protected, ensuring their continuity;
- an incident management capability is enabled to provide an effective response;
- the organization's understanding of itself and its relationships with other organizations, relevant regulators or government departments, local authorities and the emergency services is properly developed, documented and understood;
- staff are trained to respond effectively to an incident or disruption through appropriate exercising;
- stakeholder requirements are understood and able to be delivered;
- staff receive adequate support and communications in the event of a disruption;
- the organization's supply chain is secured;
- the organization's reputation is protected; and
- the organization remains compliant with its legal and regulatory obligations.

## 3.7 Elements of the business continuity management lifecycle

The BCM lifecycle comprises six elements, as illustrated by Figure 1. These can be implemented by organizations of all sizes, in all sectors: public, private, non-profit, educational, manufacturing, etc. The scope and structure of a BCM programme can vary, and the effort expended will be tailored to the needs of the individual organization, but these essential elements still have to be undertaken.

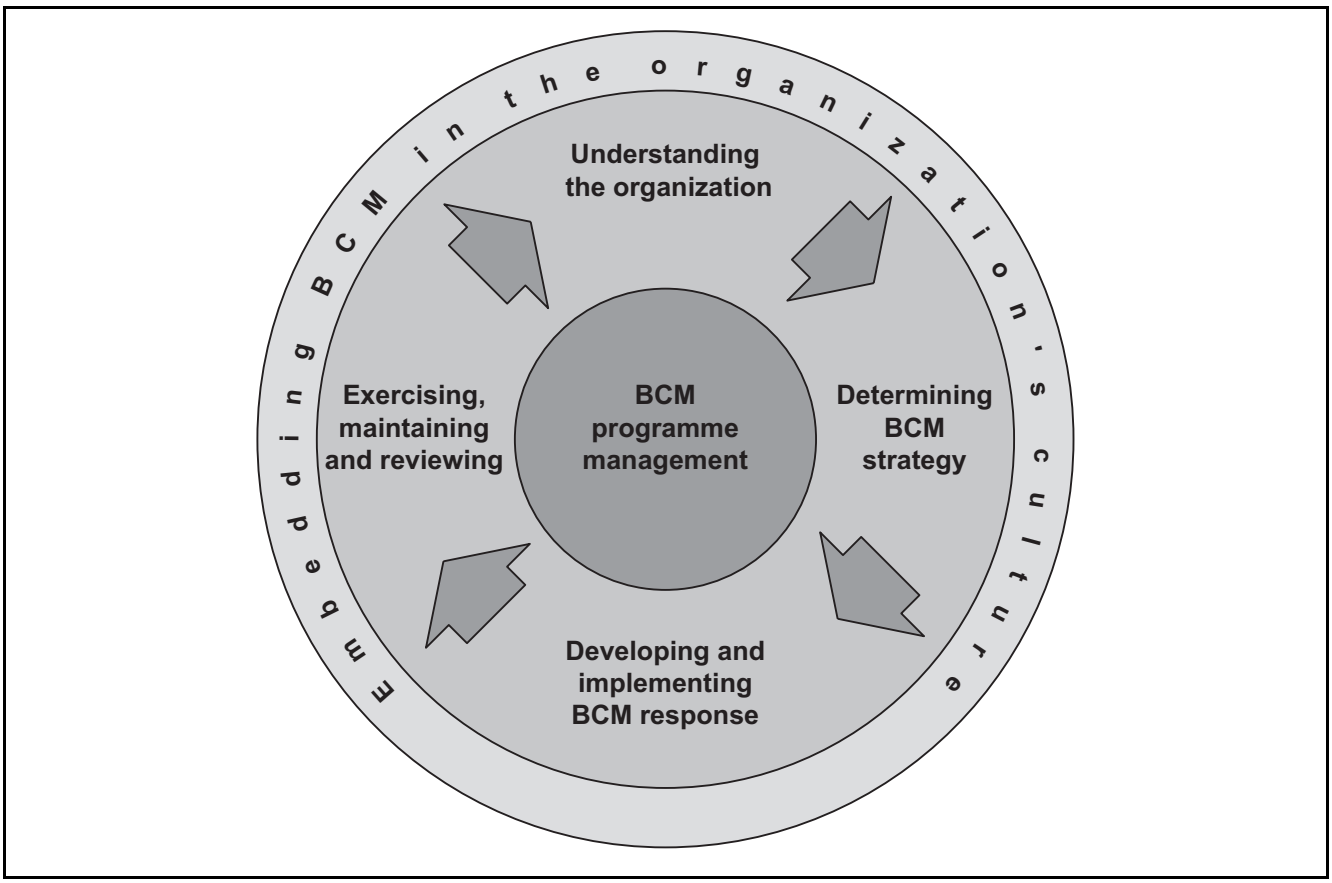
**a) BCM programme management (see** Clause **5)**

Programme management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organization.

**b) Understanding the organization (see** Clause **6)**

The activities associated with "Understanding the organization" provide information that enables prioritization of an organization's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies.

Figure 1 **The business continuity management lifecycle**




**c) Determining business continuity strategy (see** Clause **7)**

Determining business continuity strategy enables a range of strategies to be evaluated. This allows an appropriate response to be chosen for each product or service, such that the organization can continue to deliver those products and services:

- at an acceptable level of operation; and
- within an acceptable timeframe

during and following a disruption. The choice made will take account of the resilience and countermeasure options already present within the organization.

*COMMENTARY ON **3.7**d)*
*The term "incident" is used throughout this Standard to reflect the scalability of events, from small to large which can affect an organization. A single incident or series of incidents can result in serious disruptions to the organization's ability to meet its obligations. If an incident is managed well it might not develop into a crisis. However, some events will cause such a profound disruption to the organization's objectives as to be considered a crisis immediately.*

*An incident might exceed the preparedness of an organization, even if it has carefully examined response measures against an anticipated level of damage. It is therefore imperative that management and its supporting structures do not adhere stubbornly to an existing plan, but make judgments according to the circumstances. A business continuity plan is never a substitute for informed and competent management decision-making.*

**d) Developing and implementing a BCM response** (see Clause **8**)

Developing and implementing a BCM response results in the creation of a management framework and a structure of incident management, business continuity and business recovery plans that detail the steps to be taken during and after an incident to maintain or restore operations.

**e) BCM exercising, maintaining and reviewing BCM arrangements** (see Clause **9**)

BCM exercising, maintenance, review and audit leads to the organization being able to:

- demonstrate the extent to which its strategies and plans are complete, current and accurate; and
- identify opportunities for improvement.

**f) Embedding BCM in the organization's culture** (see Clause **10**)

Embedding BCM in the organization's culture enables BCM to become part of the organization's core values and instils confidence in all stakeholders in the ability of the organization to cope with disruptions.

# 4 The business continuity management policy

## 4.1 Overview

*COMMENTARY ON **4.1***
*The purposes of establishing a business continuity policy are to:*

- *ensure that all BCM activities are conducted and implemented in an agreed and controlled manner;*
- *achieve a business continuity capability that meets changing business needs and is appropriate to the size, complexity and nature of the organization; and*
- *put in place a clearly defined framework for the ongoing BCM capability.*

**4.1.1** The BCM policy defines the following processes:

- the set-up activities for establishing a business continuity capability; and
- the ongoing management and maintenance of the business continuity capability.

**4.1.2** The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability.

**4.1.3** The ongoing maintenance and management activities include embedding business continuity within the organization, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organizational structure.

## 4.2 Context

The organization should ensure that its BCM policy is appropriate to the nature, scale, complexity, geography and criticality of its business activities and that it reflects its culture, dependencies and operating environment. The BCM policy defines the process requirements to ensure that business continuity arrangements continue to meet the needs of the organization in the event of an incident. This policy should ensure that a business continuity capability is promoted within the organization's culture. The BCM capability should be integrated into the organization's change management activity so that it is incorporated into the growth and development of the organization's products and services.

## 4.3 Development of the business continuity policy

The organization should develop its business continuity policy which states the objectives of BCM within the organization. Initially, this may be a high level statement of intent which is refined and enhanced as the capability is developed.

The business continuity policy should provide the organization with documented principles to which it will aspire and against which its business continuity capability should be measured. The BCM policy should be owned at a high level, e.g. a board director or elected representative.

The organization may consider the following when developing its BCM policy:

- defining the scope of BCM within the organization;
- BCM resourcing;
- defining the BCM principles, guidelines and minimum standards for the organization;
- referencing any relevant standards, regulations or policies that have to be included or can be used as a benchmark.

The organization should maintain and regularly review its BCM policy, strategies, plans and solutions on a regular basis in line with the organization's needs.

The scope of the BCM policy should clearly define any limitations or exclusions that apply, e.g. geographical or product exclusions.

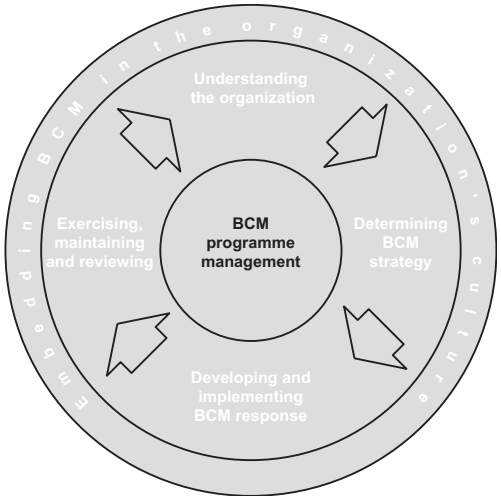
## 4.4 Scope of the BCM programme

Top management may determine the scope of the **BCM programme** by identifying the key products and services that support the organization's objectives, obligations and statutory duties. Determination of what is key should be consistent with the business impact analysis described in **6.2**, albeit at a higher level of consideration.

## 4.5 Outsourced activities

If a product, service or activity has been outsourced, the risk accountability for that product, service or activity remains vested within the organization. Consequently, an organization should assure itself that its key suppliers or outsource partners have effective BCM arrangements in place. One method of doing this is to obtain audited evidence of the viability of key suppliers' continuity plans and their exercising and maintenance programmes.

# 5 BCM programme management




Programme management is at the heart of the BCM process. Effective programme management establishes the organization's approach to business continuity.

The participation of top management is key to ensuring that the BCM process is correctly introduced, adequately supported and established as part of the organization's culture.

## 5.1 Overview

A BCM programme should be put in place to achieve the objectives defined in the business continuity policy (see **4.3**). BCM programme management involves three steps:

- assigning responsibilities (see **5.2**);
- implementing business continuity in the organization (see **5.3**); and
- the ongoing management of business continuity (see **5.4**).

## 5.2 Assigning responsibilities (governance)

**5.2.1** The organization's management should:

- appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation; and
- appoint or nominate one or more individuals to implement and maintain the BCM programme.

*COMMENTARY ON **5.2.1***

*Individuals tasked with implementing and maintaining the business continuity programme may reside in many areas of an organization depending on its size, scale and complexity. It is essential, however, that a person with appropriate authority (e.g. owner, board director or elected representative) has overall responsibility for BCM and is directly accountable for ensuring the continued success of this capability.*

**5.2.2** If the organization's structure so indicates, top management may nominate representatives across the business by function or location to assist in the implementation of the BCM programme.

The roles, accountabilities, responsibilities and authorities should be integrated into job descriptions and skill sets.

The organization's audit process should review these responsibilities.

These responsibilities may be reinforced by including them in the organization's appraisal, reward and recognition policy.

*COMMENTARY ON **5.2.2***

*In large organizations there might be a need for a team of business continuity representatives with differing roles and responsibilities. In smaller organizations, responsibility for business continuity may reside with one or more individuals.*

## 5.3 Implementing business continuity in the organization

**5.3.1** Activities to implement a business continuity programme should include the design, build, and implementation of the programme.

The organization should:

- communicate the programme to stakeholders;
- arrange or provide appropriate training for staff; and
- exercise the business continuity capability (see Clause **9**).

**5.3.2** The organization may adopt a recognized project management method to ensure that the implementation is effectively managed

## 5.4 Ongoing management

### 5.4.1 Overview

Ongoing management activities should ensure that business continuity is embedded within the organization. Each component of an organization's business continuity capability should be regularly reviewed, exercised and updated. In addition, business continuity arrangements and plans should also be reviewed and updated whenever there is a significant change in the organization's operating environment, personnel, processes or technology, and when an exercise or incident highlights deficiencies.

### 5.4.2 Ongoing maintenance

However BCM is resourced, there are activities that should be carried out both initially and on an ongoing basis. These may include:

- defining the scope, roles and responsibilities for BCM;
- appointing an appropriate person or team to manage the ongoing BCM capability;
- keeping the business continuity programme current through good practice;
- promoting business continuity across the organization and wider, where appropriate;
- administering the exercise programme;

- coordinating the regular review and update of the business continuity capability, including reviewing or reworking risk assessments and business impact analyses (BIAs);
- maintaining documentation appropriate to the size and complexity of the organization (see **5.5**);
- monitoring performance of the business continuity capability;
- managing costs associated with the business continuity capability; and
- establishing and monitoring change management and succession management regimes.

## 5.5 BCM documentation

Individuals tasked with maintaining business continuity should create and maintain the business continuity documentation. This may include the following:

a) BCM policy:
   - BCM scope statement,
   - BCM terms of reference;

b) business impact analysis (BIA);

c) risk and threat assessment;

d) BCM strategy/strategies;

e) awareness programme;

f) training programme;

g) incident management plans;

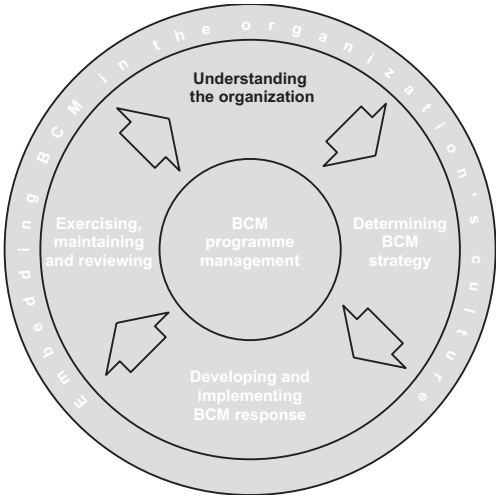
h) business continuity plans;

i) business recovery plans;

j) exercise schedule and reports;

k) service level agreements and contracts.

# 6 Understanding the organization




The aim of this element of the BCM lifecycle is to assist the understanding of the organization through the identification of its key products and services and the **critical activities** and resources that support them. This element ensures that the BCM programme is aligned to the organization's objectives, obligations and statutory duties.

## 6.1 Introduction

**6.1.1** In a business continuity context, an understanding of the organization comes from:

- identifying the organization's objectives, stakeholder obligations, statutory duties and the environment in which the organization operates;
- identifying the activities, assets and resources, including those outside the organization, that support the delivery of these products and services;
- assessing the impact and consequences over time of the failure of these activities, assets and resources (see **6.2**);
- identifying and evaluating the perceived threats that could disrupt the organization's key products and services and the critical activities, assets and resources that support them (see **6.5**).

**6.1.2** It is important that the organization understands:

a) the interdependencies of its activities, and

b) any reliance it has on external organizations, and any reliance placed upon it by others.

## 6.2 Business impact analysis (BIA)

**6.2.1** The organization should determine and document the impact of a disruption to the activities that support its key products and services. This process is commonly referred to as a business impact analysis (BIA).

**6.2.2** For each activity supporting the delivery of key products and services within the scope of its BCM programme, the organization should:

a) assess over time the impacts that would occur if the activity was disrupted;

*COMMENTARY ON **6.2.2**b)*
*During a disruption, impacts generally increase over time and affect each activity differently. Impacts might also vary depending on the day, month or point in the business lifecycle.*

b) establish the **maximum tolerable period of disruption** of each activity by identifying:

- the maximum time period after the start of a disruption within which the activity needs to be resumed,
- the minimum level at which the activity needs to be performed on its resumption,
- the length of time within which normal levels of operation need to be resumed;

c) identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

**6.2.3** When assessing impacts, the organization should consider those that relate to its business aims and objectives and its stakeholders. These may include:

- the impact on staff or public wellbeing;
- the impact of damage to, or loss of, premises, technology or information;
- the impact of breaches of statutory duties or regulatory requirements;
- damage to reputation;
- damage to financial viability;
- deterioration of product or service quality;
- environmental damage.

The organization should document its approach to assessing the impact of disruption and its findings and conclusions.

## 6.3 Identification of critical activities

*COMMENTARY ON **6.3***
*The maximum time period for resuming activities can vary between seconds and several months depending on the nature of the activity. Activities that are time-sensitive might need to be specified with a great degree of accuracy, e.g. to the minute or the hour. Less time-sensitive activities might require less accuracy.*

*The maximum tolerable period of disruption will influence each activity's **recovery time objective** when determining BCM strategies (see Clause **7**).*

The organization may categorize its activities according to their priority for recovery. Those activities whose loss, as identified during the BIA, would have the greatest impact in the shortest time and which need to be recovered most rapidly may be termed "critical activities". Each critical activity supports one or more key products or services.

The organization may wish to focus its planning activities on critical activities, but should recognize that other activities will also need to be recovered within their maximum tolerable period of disruption and might also require advance arrangements to be in place.

## 6.4 Determining continuity requirements

*COMMENTARY ON **6.4***
*Technology implies the use of equipment in the broadest sense and as relevant to the organization. Technology might include, but is not limited to, IT software and hardware, telecommunications equipment, lathes, food preparation machines, vacuum sealing machinery or any other plant and machinery essential to manufacturing and production capability.*

*If records or work-in-progress information are unavailable, inaccurate, or not sufficiently up-to-date, this could prevent or critically delay the resumption of activities. The requirements for providing such information are used to formulate appropriate back-up and records management strategies when determining BCM strategies (see Clause **7**).*

The organization should estimate the resources that each activity will require on resumption. These may include:

a) staff resources, including numbers, skills and knowledge (people);

b) the works site and facilities required (premises);

c) supporting technology, plant and equipment (technology);

d) provision of information (whether electronic or paper-based) about previous work or current work-in-progress, all of which is sufficiently up-to-date and accurate to allow the activity to continue effectively at the agreed level (information); and

e) external services and suppliers (supplies).

The organization should take into account the needs of stakeholders when determining resource levels.

## 6.5 Evaluating threats to critical activities (undertaking a risk assessment)

*COMMENTARY ON **6.5***
*It might be beneficial to consult **risk registers** that have already been established elsewhere in the organization or by external bodies.*

**6.5.1** In a BCM context, the level of risk should be understood specifically in respect of the organization's critical activities and the risk of a disruption to these. Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders. The organization should understand the threats to these resources, the vulnerabilities of each resource, and the impact that would arise if a threat became an incident and caused a business disruption.

**6.5.2** It is entirely the decision of the organization which risk assessment approach is chosen, but it is important that the approach is suitable and appropriate to address all of the organization's requirements.

**6.5.3** BS ISO/IEC 27001 sets the framework for the risk assessment approach to be chosen by describing the mandatory elements that the risk assessment process should contain. Typical elements are as follows.

- Determination of the criteria for risk acceptance. These describe the circumstances under which the organization is willing to accept risks.
- Identification of acceptable levels of risk. Whatever risk assessment approach is chosen, the organization needs to identify the levels of risk that it considers acceptable.

- Analysis of the risks. It is necessary that the organization's risk assessment approach addresses all the concepts discussed in **6.5.4**, **6.5.5** and **6.5.6**.

**6.5.4** Specific threats may be described as events or actions which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.

**6.5.5** Vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.

**6.5.6** Impacts (see **6.2.3**) might result from the exploitation of vulnerabilities by threats.

## 6.6 Determining choices

### 6.6.1 Overview

As a result of the BIA and the risk assessment**,** the organization should identify measures that:

- reduce the likelihood of a disruption;
- shorten the period of disruption; and
- limit the impact of a disruption on the organization's key products and services.

These measures are known as loss mitigation and risk treatment.

Loss mitigation strategies can be used in conjunction with other options, as not all risks can be prevented or reduced to an acceptable level. The organization might include one or more or all of the strategies in **6.6.2** to **6.6.5** for each critical activity.

### 6.6.2 Business continuity

If business continuity is the chosen strategy for a key product or service, a recovery time objective (RTO) should be established and the continuity strategies in Clause **7** should be evaluated against this objective.

Continuity strategies seek to improve the organization's resilience to a disruption by ensuring critical activities continue at, or are recovered to, an acceptable minimum level and to timeframes stipulated within the BIA.

### 6.6.3 Acceptance

A risk might be acceptable without any further action being taken. Even if it is not acceptable, the ability to do anything about some risks could be limited, or the cost of taking any action disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk if top management deems the risk to be acceptable and within the organization's risk appetite. In some circumstances the impact of a risk might be outside the organization's normal risk appetite, but, due to the low likelihood of the risk occurring and/or the uneconomic cost of control, top management may accept the risk.

Acceptance may be supplemented by a plan for handling the impacts that will arise if the risk is realized.

### 6.6.4 Transfer

For some risks the best response may be to transfer them. This might be done by conventional insurance or contractual arrangements, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. Risks may be transferred in order to reduce the risk exposure of the organization or because another organization is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable; in particular, it is generally not possible to transfer reputational risk, even if the delivery of a service is contracted out.

The purchase of insurance may form part of a risk treatment strategy and will provide some financial recompense for some losses. However, not all losses are fully insurable (e.g. uninsured incidents, damage to brand or reputation, loss of stakeholder value, reduction in market share and human consequences). A financial settlement alone is unlikely to fully protect the organization in a manner that satisfies stakeholder expectations. Insurance cover is more likely to be used in conjunction with one or more other strategies.

### 6.6.5 Change, suspend or terminate

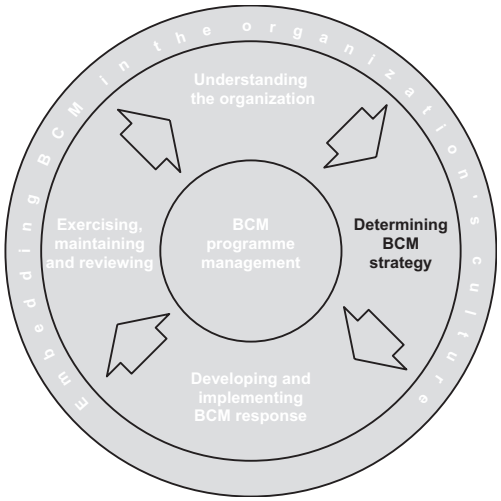
In some circumstances it might be appropriate to change, suspend or terminate the service, product, activity, function or process. This option ought only to be considered where there is no conflict with the organization's objectives, statutory compliance and stakeholder expectation. This approach is most likely to be considered where a service, product, activity, function or process has a limited lifespan.

*NOTE The four items above are sometimes referred to as the "4 T" model: "Treat" (business continuity), "Tolerate" (accept the risk), "Transfer" and "Terminate".*

## 6.7 Sign-off

**Top management** should sign off the documented list of key products and services, the business impact analysis and the risk assessment to ensure that the work has been appropriate and is a true reflection of the organization.

# 7 Determining business continuity strategy




This element of the BCM lifecycle logically follows "understanding the organization". As a result of the previous analysis, an organization will be in a position to choose the appropriate continuity strategies to enable it to meet its objectives.

## 7.1 Introduction

*COMMENTARY ON **7.1***
*Clause **7** and all following clauses relate to those key products and services for which business continuity is the chosen option. In all other cases (e.g. suspension, termination, acceptance of risk), the product or service is not covered by a BCM approach and cannot be considered compliant with this Standard.*

The organization's approach to determining BCM strategies should:

a) implement appropriate measures to reduce the **likelihood** of incidents occurring and/or reduce the potential effects of those incidents;

b) take due account of the resilience and mitigation measures;

c) provide continuity for its critical activities during and following an incident; and

d) take account of those activities that have not been identified as critical.

## 7.2 Strategy options

**7.2.1** The organization should consider strategic options for its critical activities and the resources that each activity will require on its resumption. The most appropriate strategy or strategies will depend on a range of factors such as:

- the maximum tolerable period of disruption of the critical activity;
- the costs of implementing a strategy or strategies; and
- the consequences of inaction.

**7.2.2** Strategies might be required for the following organizational resources:

- people (see **7.3**);
- premises (see **7.4**);
- technology (see **7.5**);
- information (see **7.6**);
- supplies (see **7.7**); and
- stakeholders (see **7.8**).

In each case, the organization should minimize the likelihood of implementing a business continuity solution that might be affected by the same incident that causes the business disruption.

## 7.3 People

The organization should identify appropriate strategies for maintaining core skills and knowledge. This analysis should extend beyond employees to contractors and other stakeholders who possess extensive specialist skills and knowledge. Strategies to protect or provide those skills might include:

a) documentation of the way in which critical activities are performed;

b) multi-skill training of staff and contractors;

c) separation of core skills to reduce the concentration of risk (this might entail physical separation of staff with core skills or ensuring that more than one person has the requisite core skills);

d) use of third parties;

e) succession planning; and

f) knowledge retention and management.

## 7.4 Premises

*COMMENTARY ON **7.4***
*Worksite strategies can vary significantly and a range of options might be available. Different types of incident or threat might require the implementation of different or multiple worksite options. The correct strategies will in part be determined by the organization's size, sector and spread of activities, by stakeholders, and by geographical base. For example, public authorities will need to maintain a frontline service delivery in their communities.*

The organization should devise a strategy for reducing the impact of the unavailability of its normal worksite(s). This may include one or more of the following:

a) alternative premises (locations) within the organization, including displacement of other activities;

b) alternative premises provided by other organizations (whether or not these are reciprocal arrangements);

c) alternative premises provided by third-party specialists;

d) working from home or at remote sites;

e) other agreed suitable premises; and

f) use of an alternative workforce in an established site.

*NOTE 1 If staff are to be moved to alternative premises, these premises ought to be close enough that staff are willing and able to travel there, taking into account any possible difficulties caused by the incident. However, the alternative premises ought not to be so close that they are likely to be affected by the same incident.*

*NOTE 2 The use of alternative premises for continuity purposes ought to be supported by a clear statement as to whether the alternative premises are for the sole use of the organization. If the alternative premises are shared with other organizations, a plan to mitigate the non-availability of these premises ought to be developed and documented.*

*NOTE 3 It may be appropriate to move the workload rather than the staff, e.g. a manufacturing line or a call centre's workload.*

## 7.5 Technology

*COMMENTARY ON **7.5.1***
*Technology strategies will vary significantly between organizations according to the size, nature and complexity of business. Specific strategies ought to be developed to safeguard, replace or restore specialized or custom built technologies with long lead times.*

*The organization may need to make provision for manual operations before full technology services are recovered.*

**7.5.1** Technology strategies will depend on the nature of the technology employed and its relationship to critical activities, but will typically be one or a combination of the following:

- provision made within the organization;
- services delivered to the organization; and
- services provided externally by a third party.

**7.5.2** Technology strategies may include:

- geographical spread of technology, i.e. maintaining the same technology at different locations that will not be affected by the same business disruption;
- holding older equipment as emergency replacement or spares; and
- additional risk mitigation for unique or long lead time equipment.

**7.5.3** Information technology (IT) services frequently need complex continuity strategies. Where such strategies are required, consideration should be given to:

- recovery time objectives (RTOs) for systems and applications which support the key activities identified in the BIA;
- location and distance between technology sites;
- number of technology sites;
- remote access;
- the use of un-staffed (dark) sites as opposed to staffed sites;
- telecoms connectivity and redundant routing;
- the nature of "failover" (whether manual intervention is required to activate alternative IT provision or whether this needs to occur automatically); and
- third-party connectivity and external links.

*NOTE 1 If a strategy of "failing over" from one site to another is adopted, the network path distance between the two sites has to be carefully considered as the distance between the sites could have a negative impact on the way in which IT systems operate.*

*NOTE 2 Where more than one site hosts an organization's IT, there may be a mutual IT recovery strategy, so that the systems, network and storage at each site is sized to cope with the combined traffic and work of the other(s) in addition to its own work.*

*NOTE 3 Another solution to relocating people to alternative premises is to provide them with remote access to IT via dial-up, or through the Internet using Virtual Private Network (VPN) or similar technology.*

*NOTE 4 Further guidance on continuity for IT and telecommunications hardware may be found in such documents as PAS 77, BS ISO/IEC 27001 and BS ISO/IEC 20000 (both parts).*

## 7.6 Information

Information strategies should be such as to ensure that information vital to the organization's operation is protected and recoverable according to the timeframes described within the BIA.

*NOTE 1 Further guidance is given in BS ISO/IEC 27001. The storage and recovery of such information has to be compliant with relevant legislation.*

Any information required for enabling the delivery of the organization's critical activities should have appropriate:

- confidentiality;
- integrity;
- availability; and
- currency.

Information strategies should be documented for the recovery of information that has not yet been copied or backed-up to a safe location.

- Information strategies should extend to include:
- physical (hardcopy) formats; and
- virtual (electronic) formats, etc.

*NOTE 2 In all cases, information needs to be recovered to a point in time that is known and agreed by top management. Various methods of copying may be used, such as electronic or tape backups, microfiche, photocopies, creating dual copies at the time of production and so on. This known recovery point is often referred to as the "recovery point objective".*

## 7.7 Supplies

*COMMENTARY ON 7.7*
*In office-based environments, supplies might constitute cheques, etc. Other industries might identify retail stock or just-in-time supplies, or vehicle fuels.*

**7.7.1** The organization should identify and maintain an inventory of the core supplies that support its critical activities. Strategies to provide these may include:

- storage of additional supplies at another location;
- arrangements with third parties for delivery of stock at short notice;
- diversion of just-in-time deliveries to other locations;
- holding of materials at warehouses or shipping sites;
- transfer of sub-assembly operations to an alternative location which has supplies; and
- identification of alternative/substitute supplies.

**7.7.2** Where critical activities are dependent upon specialist supplies, the organization should identify the key suppliers and single sources of supply. Strategies to manage continuity of supply may include:

- increasing the number of suppliers;
- encouraging or requiring suppliers to have a validated business continuity capability;
- contractual and/or service level agreements with key suppliers; or
- the identification of alternative, capable suppliers.

## 7.8 Stakeholders

**7.8.1** When determining appropriate BCM strategies, the organization should consider and protect the interests of its key stakeholders. These strategies should take into account relevant social and cultural considerations.

**7.8.2** The organization should identify appropriate strategies to manage relationships with key stakeholders, business or service partners and contractors. Each group might need particular considerations. Strategies to protect the interests of key stakeholders may include special arrangements for ensuring the welfare of stakeholders with specific needs, such as disability, illness or pregnancy.

**7.8.3** The organization should identify a person or persons who will discharge responsibility for welfare issues following an incident.

## 7.9 Civil emergencies

**7.9.1** Organizations seeking to determine, implement or validate strategies for incident management and business continuity management should become familiar with official local responder bodies at an early stage. These local responders are tasked with anticipation, assessment, prevention, preparation, response and recovery activities in relation to **civil emergencies** occurring within their communities.

*NOTE In the UK, these responder bodies may be known as local resilience forums.*

**7.9.2** Key responders will be instrumental in officially declaring that a civil emergency has occurred and in providing:

- pre- or post-incident advice (e.g. risk assessments);
- warning and informing procedures; and
- community recovery arrangements following a civil emergency.

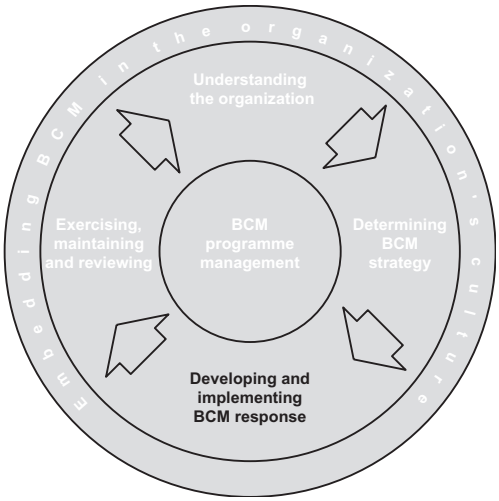
*NOTE 1 Civil emergencies can result in death and physical injury; they can have a profound and long term impact on the psychological, social, and economic welfare of individuals and their communities. Emergencies can quickly incur significant disruption to public transport services, communication networks, critical infrastructures and the smooth flow of goods, services and supplies. In light of this potential for disruption, organizations may wish to familiarize themselves with the planning arrangements of their respective local resilience forum.*

*NOTE 2 Under the UK Civil Contingencies Act (2004) [1], local authorities are lawfully required to provide business continuity advice and guidance to both commercial and voluntary organizations operating within their jurisdiction.*

## 7.10 Sign-off

Top management should sign off the documented strategies to confirm that the determination of continuity strategies has been properly undertaken and caters for likely causes and effects of disruption, and that the chosen strategies are appropriate to meet the organization's objectives within the organization's risk appetite.

# 8 Developing and implementing a BCM response




This element of the BCM lifecycle is concerned with the development and implementation of appropriate plans and arrangements to ensure continuity of critical activities, and the management of an incident.

## 8.1 Introduction

Clause **6** and Clause **7** set out how the organization should:

- identify its critical activities;
- evaluate threats to these critical activities;
- choose appropriate strategies to reduce the likelihood and impacts of incidents; and
- choose appropriate strategies that provide for the continuity or recovery of its critical activities.

The range of threats to be planned for should be determined by the organization's risk appetite.

## 8.2 Incident response structure

*COMMENTARY ON **8.2***
*In small organizations the responsibility for incident and business continuity management may be vested in a single individual. Larger organizations may use a tiered approach and may establish different teams to focus on incident management, business continuity and business recovery issues. In some cases these teams may be supported by other teams with responsibility for activities such as media communications and people issues.*

**8.2.1** The organization should define an incident response structure that will enable an effective response and recovery from disruptions.

**8.2.2** In any incident situation there should be a simple and quickly-formed structure that will enable the organization to:

- confirm the nature and extent of the incident,
- take control of the situation,
- contain the incident, and
- communicate with stakeholders.

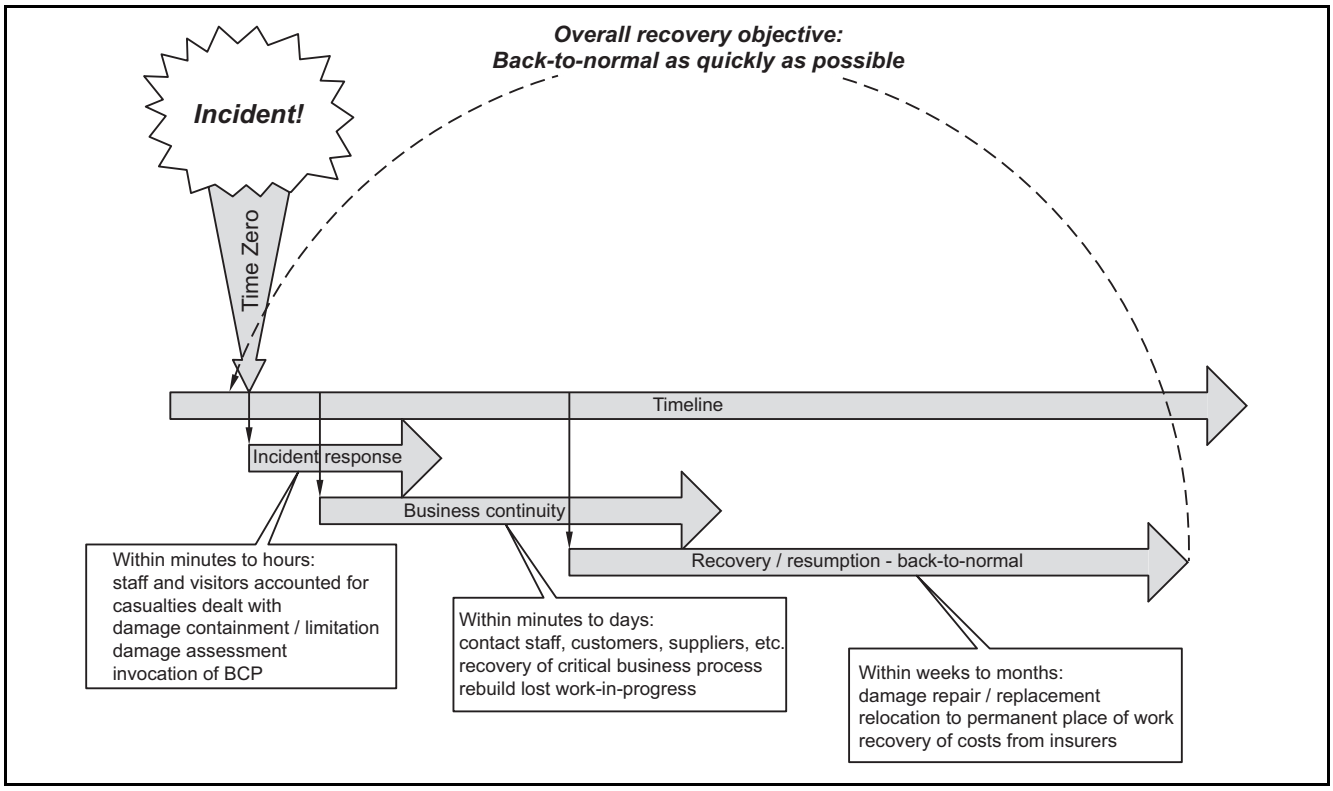
The same structure should trigger an appropriate business continuity response. This structure may be referred to as the incident management team (IMT) or crisis management team (CMT).

**8.2.3** The team should have plans, processes and procedures to manage the incident and these should be supported by business continuity tools to enable continuity and recovery of critical activities.

**8.2.4** The team should have plans for the activation, operation, coordination and communication of the incident response.

Figure 2 illustrates the three main phases over time of an incident, and the relationship between incident management and business continuity.

Figure 2 **Incident timeline**




*NOTE In some cases an organization's activation of its incident management, business continuity and business recovery plans may be enacted in rapid succession or simultaneously.*

**8.2.5** Organizations may develop specific plans to recover or resume operations back to a "normal" state (recovery plans). However, in some incidents it might not be possible to define what "normal" looks like until some time after the incident, so that it might not be possible to implement recovery plans immediately. Organizations might therefore wish to ensure that business continuity plans are capable of extended operation, giving time for the development of recovery ("back-to-normal") plans.

## 8.3 Content of plans

### 8.3.1 Introduction

*COMMENTARY ON **8.3.1***
*A small organization may have a single plan that encompasses all requirements for the business and which covers its entire operations. A very large organization may have many plans, each of which specifies in detail the recovery of:*

*— a particular part of its business;*

*— particular premises; or*

*— a particular scenario,*

*and may include separate documentation for the incident, continuity and recovery phases.*

All plans, whether incident management plans, business continuity plans or business recovery plans, should be concise and accessible to those with responsibilities defined in the plans. Plans should contain the elements in **8.3.2** to **8.3.6**.

### 8.3.2 Purpose and scope

*COMMENTARY ON **8.3.2***
*Each plan may state clearly what it does not intend to achieve and why.*

The purpose and scope of each specific plan should be defined, agreed by top management, and understood by those who will put the plan into effect. Any relationship to other relevant plans or documents within the organization should be clearly referenced and the method of obtaining and accessing these plans described.

Each incident management, business continuity and business recovery plan should set out prioritized objectives in terms of:

- the critical activities to be recovered;
- the timescales in which they are to be recovered;
- the recovery levels needed for each critical activity; and
- the situation in which each plan can be utilized.

### 8.3.3 Roles and responsibilities

*COMMENTARY ON **8.3.3***
*Plans may also contain, where appropriate, procedures and checklists that support the post-incident review process.*

The roles and responsibility of the people and teams having authority (both in terms of decision-making and authority to spend) during and following an incident should be clearly documented.

The persons or groups covered by a plan should be clearly defined.

### 8.3.4 Plan invocation

*COMMENTARY ON **8.3.4***
*Time lost during a response can never be regained. It is almost always better to mobilize the response team and subsequently stand it down than to miss an opportunity to contain an incident early and prevent escalation.*

*Organizations may factor in defined and internationally agreed escalation stages in line with clear guidance from other expert sources, e.g. the World Health Organization for pandemics.*

The method by which an incident management, business continuity or business recovery plan is invoked should be clearly documented. This process should allow for the relevant plans or parts thereof to be invoked in the shortest possible time following the occurrence of a business disruption.

The organization should establish and document clear guidelines and a set of criteria regarding which individual(s) have the authority to invoke the plan(s) and under what circumstances.

The invocation process may require the immediate mobilization of organizational resources. The plan should include a clear and precise description of:

- how to mobilize the team(s);
- immediate rendezvous points; and
- subsequent team meeting locations and details of any alternative meeting locations (in larger organizations, these meeting places may be referred to as incident management or command centres).

The organization should document a clear process for standing down the team(s) once the incident is over, and returning to business as usual.

### 8.3.5 Document owner and maintainer

The organization should nominate the primary owner of the plan, and identify and document who is responsible for reviewing, amending and updating the plan at regular intervals.

A system of version control should be employed, and changes formally notified to all interested parties with a formal plan distribution record maintained and kept up-to-date.

### 8.3.6 Contact details

*COMMENTARY ON **8.3.6***
*The contact records may include "out of hours" contact details. However, where plans reference such private details, respect for data protection has to be a paramount consideration.*

Each plan should contain or provide a reference to the essential contact details for all key stakeholders.

## 8.4 The incident management plan (IMP)

The purpose of an IMP is to allow the organization to manage the initial (acute) phase of an incident.

The IMP should:

a) be flexible, feasible, and relevant;

b) be easy to read and understand; and

c) provide the basis for managing all possible issues, including the stakeholder and external issues, facing the organization during an incident.

The IMP should also:

1) have top management support, including a board sponsor where applicable; and
2) be supported by an appropriate budget for development, maintenance and training.

## 8.5 Contents of the IMP

### 8.5.1 General

In addition to the content recommended in **8.3**, an IMP should include the information in **8.5.2** to **8.5.8**.

### 8.5.2 Task and action lists

The IMP should include task lists and action checklists to manage the immediate consequences of a business disruption. These tasks should:

- ensure that safety of individuals is addressed first;
- be based upon the results of the organization's BIA;
- be structured in a way that delivers the strategic and tactical options chosen by the organization (as described in Clause **7**); and
- help prevent the further loss or unavailability of critical activities, and supporting resources as defined in Clause **7**.

### 8.5.3 Emergency contacts

*COMMENTARY ON **8.5.3***
*Depending upon the scale of the organization and the size of the incident, a number of competent, trained people may be required to respond to telephone enquiries about the incident.*

A description of how, and under what circumstances, the organization will communicate with staff and their relatives, friends and emergency contacts should be included. In some cases, it might be appropriate to include detail in a separate document.

Next-of-kin and emergency contact information for all personnel should be kept up-to-date and available for prompt use.

### 8.5.4 People activities

*COMMENTARY ON **8.5.4***
*Organizations have a direct responsibility to safeguard the welfare of employees, contractors, visitors and customers where an incident poses a direct risk to life, livelihood and welfare. Special attention will need to be paid to any groups with disabilities or other specific needs (e.g. pregnancy, temporary disability due to injury, etc.). Planning in advance to meet these requirements can reduce risk and reassure those affected.*

*The long-term impacts of incidents cannot be underestimated. Developing appropriate strategies in support of human welfare can directly promote physical and emotional recovery within the organization.*

The IMP should satisfy the interests of those whose welfare might be put at risk as a result of an incident, taking into account relevant social and cultural considerations (see **7.8.2**).

The IMP should identify the person(s), who will discharge responsibility for welfare issues following an incident (see **7.8.3**), including:

a) site evacuation (inclusive of internal "shelter-at-site" activities);
b) the mobilization of safety, first aid or evacuation-assistance teams;
c) locating and accounting for those who were on site or in the immediate vicinity;
d) ongoing employee/customer communications and safety briefings.

The organization should deploy staff with appropriate levels of authority to liaise where appropriate with the emergency services.

*NOTE Emergency services play the primary role in protecting life and relieving suffering during emergencies. Therefore, early liaison, pre-planning and real-time incident coordination between the organization and its first responders and the emergency services can improve the efficiency of an incident response.*

The organization may retain a means to provide services to debrief and counsel affected staff after an incident. Services may be sourced externally or may be provided as an extension to existing occupational health and employee assistance programmes.

### 8.5.5 Media response

*COMMENTARY ON **8.5.5***
*Pre-prepared information can be especially useful in the early stages of an incident. It enables an organization to provide details about the organization and its business while details of the incident are still being established. An organization may use all applicable means to share information during and after an incident. Such sources may include websites, spokespeople, news sources, and generic company briefing statements.*

The organization's media response should be documented in the IMP, including:

a) the incident communications strategy;

b) the organization's preferred interface with the media;

c) a guideline or template for the drafting of a statement to be provided to the media at the earliest practicable opportunity following the incident;

d) appropriate numbers of trained, competent, spokespeople nominated and authorized to release information to the media;

e) establishment, where practicable, of a suitable venue to support liaison with the media, or other stakeholder groups.

In some cases, it may be appropriate to:

- provide supporting detail in a separate document;
- establish an appropriate number of competent, trained people to answer telephone enquiries from the press;
- prepare background material about the organization and its operations (this information should be pre-agreed for release);
- ensure that all media information is made available without undue delay.

### 8.5.6 Stakeholder management

*COMMENTARY ON **8.5.6***
*Pressure or community action groups who collectively have power or influence over the organization might also need to be considered.*

A process for identifying and prioritizing communications with other key stakeholders should be included. It may be necessary to develop a separate stakeholder management plan to provide criteria for setting priorities and allocating a person to each stakeholder or group of stakeholders.

### 8.5.7 Incident management location

*COMMENTARY ON **8.5.7***
*An incident management location provides a known focal point from which the incident can be managed. It is important to capture and share key information and to set objectives, assign tasks, manage resources, identify and track issues, and make informed decisions. Good communications are essential. The use of a meeting point overcomes the situations where telephone networks are overloaded.*

*The location may be as simple as a hotel room or a staff member's house. It may be as complex as a dedicated "command centre" with PCs, video-conferencing and multiple telephones.*

*Initially, it might be necessary to hold a virtual or off-site meeting, e.g. via telephone, teleconference or videoconference, so that key decisions can be made promptly.*

The organization should define a robust and predetermined location, room or space from which an incident will be managed. Once established, this location should be the focal point for the organization's response. An alternative meeting point at a different location should also be nominated in case access to the primary location is denied. Each location should have access to appropriate resources by which the incident team may initiate effective incident management activities without delay.

The chosen location should be fit-for-purpose and include:

a) effective primary and secondary means of communication;

b) facilities for accessing and sharing information, including the monitoring of the news media.

### 8.5.8 Annexes

The IMP should include up-to-date contact and mobilization details for any relevant agencies, organizations and resources that might be required to support the organization's response strategies.

The IMP should include logs or forms for the recording of vital information about the incident, such as the incident timeline, details of casualties, decisions made, money spent, details of casualties, damage assessments, communications issued, and all other information deemed essential by the organization to support post incident review.

The IMP may also include or reference:

a) maps, charts, plans, photographs and other information that might be relevant in the event of an incident;

b) documented response strategies agreed with third parties as appropriate (joint venture partners, contractors, suppliers, etc.);

c) details of equipment storage and staging areas;

d) site access plans; and

e) a claims management procedure that ensures all insurance and legal claims for or against the organization meet regulatory and contractual requirements.

## 8.6 The business continuity plan(s) [BCP(s)]

*COMMENTARY ON **8.6***
*The components and contents of BCPs vary from organization to organization and have a different level of detail based on the scale, environment, culture and technical complexity of the organization.*

*Large organizations might require separate documents for each of their critical activities, whereas smaller organizations might be able to cover everything that is critical to them within a single document.*

The purpose of a business continuity plan (BCP) is to enable an organization to recover or maintain its activities in the event of a disruption to normal business operations.

BCPs are activated (invoked) to support the critical activities required to deliver the organization's objectives. They may be invoked in whole or part and at any stage of the response to an incident.

## 8.7 Contents of the BCP

### 8.7.1 General

In addition to the items recommended in **8.3**, a BCP should contain the elements in **8.7.2** to **8.7.5**.

### 8.7.2 Action plans/ task lists

*COMMENTARY ON **8.7.2***
*These points are consistent with the requirements of the Civil Contingencies Act [1], Section 6.20.*

*Plans will reference the people, premises, technology, information, supplies and stakeholders identified in the strategies phase (see Clause **7**). Clear assumptions and details of any resources required to implement plans ought to be included. In the event that the lack of a service or resource makes the plan's goals unachievable, a clear procedure for escalating the issue ought to be defined.*

The action plan should include a structured checklist of actions and tasks in an order of priority, highlighting:

a) how the BCP is invoked;

b) the person(s) responsible for invoking the business continuity plan;

c) the procedure that person should adopt in taking that decision;

d) the person(s) who should be consulted before such a decision is taken;

e) the person(s) who should be informed once a decision has been taken;

f) who goes where, and when;

g) what services are available where, and when; including how the organization mobilizes external and third-party resources;

h) how and when this information is communicated; and

i) if relevant, detailed procedures for manual workarounds, system recovery, etc.

### 8.7.3 Resource requirements

The resources required for business continuity and business recovery should be identified at different points in time. These may include:

a) people, which may include:
   - security,
   - transportation logistics,
   - welfare needs, and
   - emergency expenses;

b) premises;

c) technology, including communications;

d) information, which may include:
   - financial (e.g. payroll) details,
   - customer account records,
   - supplier and stakeholder details,
   - legal documents (e.g. contracts, insurance policies, title deeds, etc.), and
   - other services documents (e.g. service level agreements);

e) supplies; and

f) management of, and communication with, stakeholders.

### 8.7.4 Responsible person(s)

*COMMENTARY ON **8.7.4***
*In many cases the organization may wish to nominate the same individual(s) identified in the incident management plan and direct them to manage the longer-term issues.*

The organization should identify a nominated person(s) to manage the business continuity and business recovery phases of a disruption.

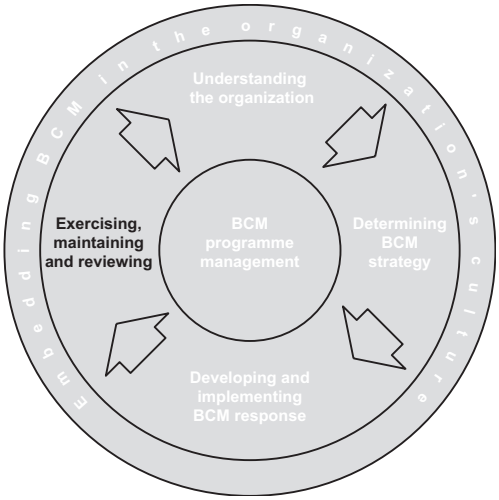
### 8.7.5 Forms and annexes

*COMMENTARY ON **8.7.5***
*The plan may also include forms for recording administrative data, e.g. resources used, expenses recording materials; maps, drawings, and site and office plans, especially those relating to any alternative facilities such as workspace recovery areas and storage locations.*

Where appropriate, the BCP should contain up-to-date contact details for relevant internal and external agencies, organizations and providers that might be required to support the organization.

The business continuity plan should include an incident log or forms for the recording of vital information, especially in respect of decisions made.

# 9 Exercising, maintaining and reviewing BCM arrangements




This element of the BCM lifecycle ensures that an organization's BCM arrangements are validated by exercise and review and that they are kept up-to-date.

## 9.1 Introduction

An organization's business continuity and incident management arrangements cannot be considered reliable until exercised and unless their currency is maintained. Exercising is essential to developing teamwork, competence, confidence and knowledge which is vital at the time of an incident.

Arrangements should be verified through exercising, audit and self-assessment processes to ensure that they are fit-for-purpose.

## 9.2 Exercise programme

*COMMENTARY ON **9.2***
*Exercises provide demonstrable evidence of a business continuity and incident management competence and capability. Time and resources spent proving BCM strategies by exercising BCPs will lead to a fit-for-purpose capability. No matter how well designed and thought-out a BCM strategy or BCP appears to be, a series of robust and realistic exercises will identify areas that require amendment.*

An exercise programme should be consistent with the scope of the business continuity plan(s), giving due regard to any relevant legislation and regulation. Exercises may:

- anticipate a predetermined outcome, e.g. are planned and scoped in advance; or
- allow the organization to develop innovative solutions.

An exercise programme should be devised that, over a period of time, leads to objective assurance that the BCP will work as anticipated when required. The programme should:

- exercise the technical, logistical, administrative, procedural and other operational systems of the BCP;
- exercise the BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.);
- validate the technology and telecommunications recovery, including the availability and relocation of staff.

In addition, it might lead to the improvement of BCM capability by:

- practising the organization's ability to recover from an incident;
- verifying that the BCP incorporates all organizational critical activities and their dependencies and priorities;
- highlighting assumptions which need to be questioned;
- instilling confidence amongst exercise participants;
- raising awareness of business continuity throughout the organization by publicizing the exercise;
- validating the effectiveness and timeliness of restoration of critical activities; and
- demonstrating competence of the primary response teams and their alternatives.

## 9.3 Exercising BCM arrangements

**9.3.1** Exercises should be realistic, carefully planned, and agreed with stakeholders, so that there is minimum risk of disruption to business processes. An exercise should be planned such that the risk of an incident occurring as a direct result of the exercise is minimized.

**9.3.2** Every exercise should have clearly defined aims and objectives. A post-exercise debriefing and analysis should be undertaken which considers the achievement of the aims and objectives of the exercise. A post-exercise report should be produced that contains recommendations and a timetable for their implementation.

**9.3.3** The scale and complexity of exercises should be appropriate to the organization's recovery objectives.

**9.3.4** Business continuity and incident management plans should be exercised to ensure that they can be executed correctly, and contain appropriate detail and instructions.

*COMMENTARY ON **9.3.4***
*Exercises that show serious deficiencies or inaccuracies in the BCP ought to be rerun after corrective actions have been completed.*

*A range of approaches to exercising BCM strategies is shown in Table 1.*

Table 1 **Types and methods of exercising BCM strategies**

| Complexity | Exercise | Process | Variants | Good practice frequency [A)] |
|---|---|---|---|---|
| Simple | Desk check | Review/amendment of content<br>Challenge content of BCP | Update/validation<br>Audit/verification | At least annually<br>Annually |
| Medium | Walk-through of plan | Challenge content of BCP | Include interaction and validate participants' roles | Annually |
| | Simulation | Use "artificial" situation to validate that the BCP(s) contains both necessary and sufficient information to enable a successful recovery | Incorporate associated plans | Annually or twice yearly |
| | Exercise critical activities | Invocation in a controlled situation that does not jeopardize business as usual operation | Defined operations from alternative site for a fixed time | Annually or less |
| Complex | Exercise full BCP, including incident management | Building-/ campus-/ exclusion zone-wide exercise | | Annually or less |

[A)] The frequency of exercises should depend upon both the organization's needs, the environment in which it operates, and stakeholder requirements. However, the exercising programme should be flexible, taking into account the rate of change within the organization and the outcome of previous exercises. The above exercise methods can be employed for individual plan components, and single and multiple plans.

**9.3.5** The exercise programme should consider the roles of all parties, including key third party providers, outsource partners and others who would be expected to participate in recovery activities. An organization may include such parties in its exercises.

## 9.4 Maintaining BCM arrangements

*COMMENTARY ON **9.4***
*The purpose of the BCM maintenance process is to ensure that the organization's BCM competence and capability remains effective, fit-for purpose and up-to-date.*

*Maintenance activities ought to modify existing exercise schedules when they indicate that there has been a significant change in the strategy, solution or business process.*

A clearly defined and documented BCM maintenance programme should be established. This programme should ensure that any changes (internal or external) that impact the organization are reviewed in relation to BCM. It should also identify any new products and services and their dependent activities that need to be included in the BCM maintenance programme.

As a result of the BCM maintenance programme, the organization should:

- review and challenge any assumptions made in any components of BCM throughout the organization; and
- distribute updated, amended or changed BCM policy, strategies, solutions, processes and plans to key personnel under a formal change control process.

*NOTE If there are major business changes then a revision of the BIA ought to be undertaken. The other components of the BCM programme may be amended to take account of these changes.*

The outcomes from the BCM maintenance process should include:

- documented evidence of the proactive management and governance of the organization's business continuity programme;
- verification that key people who are to implement the BCM strategy and plans are trained and competent;

- verification of the monitoring and control of the BCM risks faced by the organization; and
- documented evidence that material changes to the organization's structure, products and services, activities, purpose, staff and objectives have been incorporated into the organization's business continuity and incident management plans.

## 9.5 Reviewing BCM arrangements

**9.5.1** The organization's top management should, at intervals that it deems appropriate, review the organization's BCM capability, to ensure its continuing suitability, adequacy and effectiveness. This review should be documented.

**9.5.2** The review should verify that compliance with the organization's BCM policy ensures compliance with any applicable laws, standards, strategies, frameworks and good practice guidelines.

*COMMENTARY ON **9.5.3***
*In the context of continual improvement, the organization may acquire knowledge on new BCM-related technology and practices, including new tools and techniques, and these have to be evaluated to establish their potential benefit to the organization.*

**9.5.3** The review should address the possible need for changes to policy, strategy, objectives and other elements of the BCM management system in the light of such things as exercise results, changing circumstances and the commitment to continual improvement.

**9.5.4** The review can take the form of internal or external audits, or self-assessments. The frequency and timing of reviews can be influenced by laws and regulations, depending on the size, nature and legal status of the organization. They might also be influenced by the requirements of stakeholders.

An audit or self-assessment of the organization's BCM programme should verify that:

- all key products and services and their supporting critical activities and resources have been identified and included in the organization's BCM strategy;
- the organization's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the organization's objectives);
- the organization's BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- the organization's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the organization;
- the organization's BCM maintenance and exercising programmes have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance programme;
- the organization has an ongoing programme for BCM training and awareness;
- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- change control processes are in place and operate effectively.

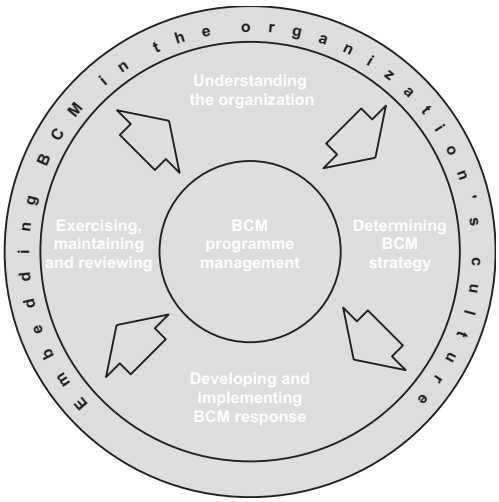
### 9.5.5 Audit

The organization should provide for the independent audit of its BCM competence and capability to identify actual and potential shortcomings. It should establish, implement and maintain procedures for dealing with these. Independent audits should be conducted by competent persons, whether internal or external.

### 9.5.6 Self-assessment

A BCM self-assessment process plays a role in ensuring that an organization has a robust, effective and fit-for-purpose BCM competence and capability. It provides the qualitative verification of an organization's ability to recover from an incident. Self-assessment should be conducted against the organization's objectives. It should also take into account relevant industry standards and good practice.

# 10 Embedding BCM in the organization's culture




To be successful, business continuity has to become part of the way that an organization is managed, regardless of size or sector. At each stage of the BCM process, opportunities exist to introduce and enhance an organization's BCM culture.

## 10.1 General

*COMMENTARY ON **10.1***
*Creating and embedding a BCM culture within an organization can be a lengthy and difficult process which might encounter a level of resistance that was not anticipated. An understanding of the existing culture within the organization will assist in the development of an appropriate BCM culture programme.*

*All staff have to understand that BCM is a serious issue for the organization and that they have an important role to play in maintaining the delivery of products and services to their clients and customers.*

Building, promoting and embedding a BCM culture within an organization ensures that it becomes part of the organization's core values and effective management.

An organization with a positive BCM culture will:

- develop a BCM programme more efficiently;
- instil confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions;
- increase its resilience over time by ensuring BCM implications are considered in decisions at all levels; and
- minimize the likelihood and impact of disruptions.

Development of a BCM culture is supported by:

- leadership from senior personnel in the organization;
- assignment of responsibilities (see **5.2**);
- awareness raising;
- skills training; and
- exercising plans.

## 10.2 Awareness

*COMMENTARY ON **10.2***
*Raising and maintaining awareness of BCM with all the organization's staff is important to ensure that they are aware of why BCM is important to the organization. They will need to be shown that this is a lasting initiative that has the ongoing support of top management.*

The organization should have a process for identifying and delivering the BCM awareness requirements of the organization and evaluating the effectiveness of its delivery.

BCM staff should make themselves aware of external BCM information. This may be done in conjunction with seeking guidance from emergency services, local authorities and regulators.

The organization should raise, enhance and maintain awareness by maintaining an ongoing BCM education and information programme for all staff.

Such a programme may include:

- a consultation process with staff throughout the organization concerning the implementation of the BCM programme;
- discussion of BCM in the organization's newsletters, briefings, induction programme or journals;
- inclusion of BCM on relevant web pages or intranets;
- learning from internal and external incidents;
- BCM as an item at team meetings;
- exercising continuity plans at an alternative location (e.g. a recovery site); and
- visits to any designated alternative location (e.g. a recovery site).

The organization may extend its BCM awareness programme to its suppliers and other stakeholders.

## 10.3 Skills training

The organization should have a process for identifying and delivering the BCM training requirements of relevant participants and evaluating the effectiveness of its delivery.

The organization should undertake training of:

a) BCM staff for tasks such as:

- BCM programme management,
- conducting a business impact analysis,
- developing and implementing BCPs,
- running a BCP exercise programme,
- risk and threat assessment, and
- media communications;

b) non-BCM staff requiring skills to undertake their nominated roles in incident response or business recovery.

Response skills and competence throughout the organization should be developed by practical training, including active participation in exercises.

# References

## Standards publications

BS EN ISO 9000, *Quality management systems – Fundamentals and vocabulary*

BS ISO/IEC 20000 (both parts), *Information technology – Service management*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

PAS77, *IT Service Continuity Management*

## Other publications

[1] The Civil Contingencies Act 2004, London: TSO

*This page deliberately left blank*

# BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

### Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

### Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

### Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111.
Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002.
Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

### Copyright




389 Chiswick High Road
London
W4 4AL