British Standard

PAS 56

Guide to Business Continuity Management

ICS 03.100.01

BCI
The Business Continuity Institute

Insight
Consulting

BSI

This Publicly Available Specification comes into effect on 24 March 2003

ISBN 0 580 41370 5

Amd. No.	Date	Comments

Contents

Foreword

This Publicly Available Specification, PAS 56, was sponsored by the Business Continuity Institute[1] and Insight Consulting Limited[2], and developed through the British Standards Institution.

Acknowledgement is given to the following organizations that were consulted in the development of this Publicly Available Specification:

Adviza Risk Management

Corporation of London

Electronic Data Systems Corporation

Insight Consulting Limited

Marsh UK Ltd

Office of Government Commerce

Post Office Ltd

Redan International/CMA

Royal & SunAlliance

Sainsburys

The Business Continuity Institute

This Publicly Available Specification is based upon the Business Continuity Institute's *Business Continuity Management*: *Good Practice Guidelines, 2002* [1].

The steering group of this Publicly Available Specification wishes to acknowledge the personal contributions of John Bartlett and Dr David J Smith FBCI to the development of the document.

This Publicly Available Specification (PAS) is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

Compliance with a Publicly Available Specification does not in itself confer immunity from legal obligations.

[1)] The Business Continuity Institute, PO Box 4474, Worcester WR6 5YA; telephone 08706 038783; www.thebci.org
[2)] Insight Consulting Limited, Churchfield House, 5 The Quintet, Churchfield Road, Walton on Thames, Surrey KT12 2TZ; telephone 01932 241000; www.insight.co.uk

Introduction

Business continuity management (BCM) should be a fit-for-purpose, business-owned and -driven activity that unifies a broad spectrum of business and management disciplines in both the public and private sectors, including crisis management, risk management and technology recovery, and should not be limited to information technology disaster recovery (ITDR) (see Figure 1). BCM is directly linked to corporate governance and establishes good management practice.

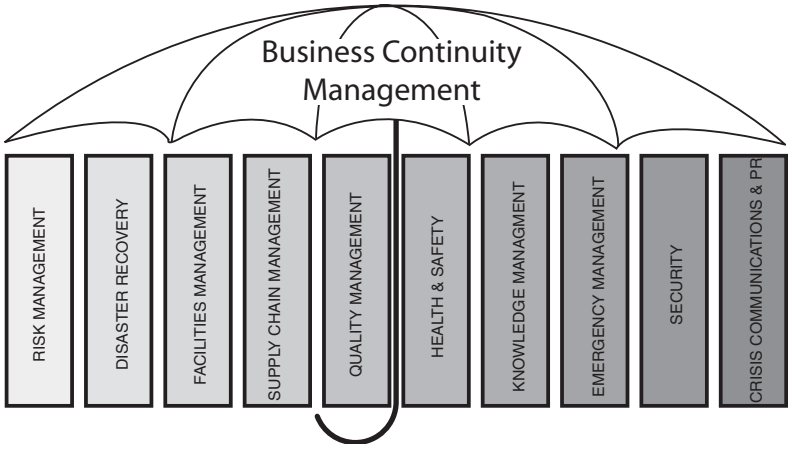

Figure 1 — BCM — the unifying process[3]

BCM establishes a strategic and operational framework to implement, proactively, an organization's resilience to disruption, interruption or loss in supplying its products and services. It should not purely be a reactive measure taken after an incident has occurred. BCM requires planning across many facets of an organization (see Figure 2); therefore its resilience depends equally on its management and operational staff, as well as technology, and requires a holistic approach to be taken when establishing a BCM programme.

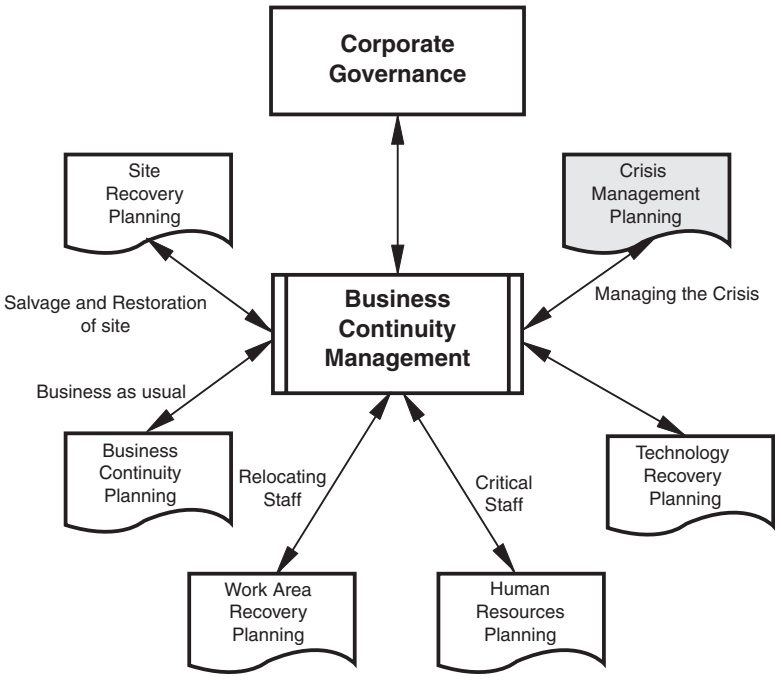

Figure 2 — BCM relationships[4]

[3] Source: Adapted from Smith, 2002 [1]
[4] Source: Adapted from Smith, 2001 [2]; and Smith, 2002 [1]

Many organizations believe that incidents will not happen to them, or that insurance alone will enable them to recover effectively from a loss or incident. Insurance is a key component of an overall BCM solution. However, while it may provide for the financial aspects of a loss or incident, insurance does not provide a method to prevent an incident or recover and rebuild an organization or win back customer confidence.

Whilst bombs, fires and floods capture the headlines, most crises are "quiet catastrophes" that only affect an individual organization. These quiet catastrophes have the potential to damage an organization's most valuable assets i.e. its brand or public image and its reputation. Image and reputation can be destroyed very quickly unless vigorously defended at a time when the speed and scale of events can overwhelm the normal operational and management systems. Effective BCM demonstrates this competence and capability and enables an organization to return to normal.

This PAS is aimed at the person responsible for implementing, delivering and managing BCM within an organization (the "BCM manager").

> **NOTE** It is recognized that in smaller organizations this can often be part of a person's wider role.

It is designed to provide assistance to the BCM manager in understanding and implementing a BCM programme. Each BCM manager will need to assess the application of the guidelines given in this PAS to their own organization and ensure that its BCM competence and capability meets the nature, scale, complexity, geography and criticality of its business activities and reflects its individual culture and operating environment.

All organizations depend upon others to enable the delivery of their products and services to customers and clients (the supply chain). As a result, BCM applies across industry sectors and cultural divides. The development of this PAS is seen as essential to achieve an effective and consistent BCM programme. It aims to provide a generic framework and guidelines for BCM.

This PAS focuses on each of the six stages of the BCM life-cycle and process.

1 Scope

This PAS establishes the process, principles and terminology of BCM, describes the activities and outcomes involved, provides recommendations for good practice and outlines evaluation criteria. It is applicable to all organizations, regardless of size or industry sector.

2 Terms and definitions

For the purposes of this PAS the following terms and definitions apply.

2.1
assurance

activity and process whereby an organization can verify and validate its BCM capability

2.2
backlog processing

the processing of work that has built up due to a disruption in a mission critical activity (MCA)

2.3
business continuity management (BCM)

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

2.4
business continuity planning

advance planning and preparation which is necessary to identify the impact of potential losses, to formulate and implement viable continuity strategies, and to develop continuity plan(s) which ensure continuity of organizational services in the event of an incident

> **NOTE** The deliverable from business continuity planning is a business continuity plan (BCP) which is a documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident.

2.5
business impact analysis (BIA)

management analysis by which an organization assesses the quantitative (e.g. financial, service levels) and qualitative (e.g. operational, reputational, legal, regulatory) impacts and loss that might result if that organization were to suffer a major incident, and the minimum level of resource required for recovery (business impact resource recovery analysis [BIRRA])

> **NOTE** The findings from a BIA are used to make decisions and justify a business continuity planning strategy and solution.

2.6

business response work area

work space shared by a limited number of organizations that require facilities to be obtained and installed for recovery

2.7
business risk

risk that internal and external factors, such as inability to provide a service or product, or a fall in demand for an organizations products or services, will result in unexpected loss

2.8
corporate governance

system by which the directors and officers of an organization are required to carry out their accountabilities and responsibilities for ensuring that effective management systems, including financial monitoring and control systems, have been put in place to protect assets, earning capacity and the reputation of the organization

> **NOTE** For example, all UK listed companies on the London Stock Exchange are required to comply with corporate governance code of conduct.

2.9
crisis management

process by which an organization manages the wider impact of any incident until it is either under control or contained without impact to the organization or until the BCP is invoked

2.10
dedicated work area

work space provided for sole use by a single organization, configured ready for use

2.11
emergency response

initial response to any incident, focused on protecting human life and the organization's assets

2.12
end-to-end

in entirety, from start to finish

2.13
exclusion zone

geographical zone agreed between a client and a third party provider of work area recovery (WAR) resources within which the third party provider will not provide WAR services to another client

2.14
exercising

the critical testing of BCM strategies and BCPs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g. technology, telephony, administration) to demonstrate BCM competence and capability

> **NOTE** An exercise may 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 may arise, prior to a real invocation.

2.15

fit for purpose

meeting an organization's requirements

2.16
incident

a situation that may be, or may lead to, a business interruption, disruption, loss, emergency or crisis

2.17
just-in-time supply chain (JIT)

system whereby dependencies for MCAs are provided when required, without requiring storage

2.18
key performance indicator (KPI)

benchmark measurement based on objectives, targets and defined industry standards

2.19
level of business continuity (LBC)

minimum level of continued output of products and/or services acceptable to an organization in achieving its business objectives

NOTE LBC can be influenced or dictated by regulation or legislation.

2.20
mission critical activity (MCA)

critical operational and/or business support, service or product related activity (provided internally or externally), including its dependencies and single points of failure, which enables an organization to achieve its business objective(s), taking into account seasonal trends and/or critical timing issues

2.21
mobile recovery solution

work space (normally syndicated) transported to a location specified by an organization for the purposes of work area recovery

2.22
operational risk

risk that deficiencies in information systems or internal controls will result in unexpected loss

NOTE This risk is associated with human error, system failures and inadequate procedures and controls.

2.23
performance measure

an indicator used to quantify efficiency and/or effectiveness

NOTE An example of a performance measure is a KPI.

2.24
reciprocal agreement

two-way arrangement by which organizations agree to use each other's resources in the event of a business continuity incident

2.25

reciprocal work area

work space provided by one organization for use by another in the event of a business continuity incident, by way of a reciprocal agreement (**2.24**)

2.26
recovery point objective (RPO)

point in time to which work should be restored following a business continuity incident that interrupts or disrupts an organization

NOTE For example, this may be "start of day".

2.27
recovery time objective (RTO)

time scale in which MCAs must be recovered

2. 28
residual risk

level of risk remaining after all cost-effective actions have been taken to lessen the impact, probability and consequences of a specific risk or group of risks, subject to an organization's risk appetite

2.29
resilience

ability of an organization, staff, system, telecommunications network, activity or process to absorb the impact of a business interruption, disruption or loss and continue to provide a minimum acceptable level of service

2.30
resiliency measure

activity or facility put in place to absorb the impact of an interruption, disruption or loss and to continue to provide a minimum acceptable level of service

2.31
resource recovery solution

plan of action that identifies the specific resource required to carry out recovery actions

2.32
response

action taken to address an incident in order to assess the level of containment and control activity required

2.33
risk

chance of something happening, measured in terms of impact and probability

> **NOTE** The consequence may be either positive or negative. Risk in a general sense can be defined as the threat of an action or inaction that will prevent an organization's ability to achieve its business objectives.

2.34
risk appetite

willingness of an organization to accept a defined level of risk

> **NOTE** Different organizations at different stages of their existence will have different risk appetites.

2.35
risk assessment (RA)

overall process of risk identification, analysis and evaluation

2.36
risk concentration

concentration of MCAs within the same building or on the same site

2.37
risk management

establishment of culture, processes and structures to manage potential opportunities and adverse effects

> **NOTE** As it is not possible or desirable to eliminate all risk, the objective is to implement cost-effective processes that reduce risks to an acceptable level, reject unacceptable risks and treat risk by financial interventions, i.e. transfer other risks through insurance or other means, or by organizational intervention i.e. BCM.

2.38

risk management programme

set of controls, processes and structures put in place to support risk management

2.39
risk profile

collection of risks that an organization faces

2.40
single point of failure

sole source of a service, activity or process, i.e. to which there is no alternative, the failure of which would lead to the total failure of an MCA

2.41
strategy

vision and direction for an organization, involving the setting of mission statements and identifying markets and objectives so that the *raison d' être* of the organization can be achieved

2.42

syndicated or shared subscription work area

work space shared by a limited number of organizations, configured for general occupation (not for a particular organization)

2.43
syndication ratio

number of times that a work area is sold by the third party providers at a resource recovery location

> **NOTE** A work area's availability at the time of business continuity incident could be on a first-come-first-served basis or a reduced allocation basis.

2.44
vital records

records (all media) which are considered to be essential to the continuation of an organization's business

2.45
work area recovery (WAR)

provision of (internal or external) pre-designated work space providing the minimum necessary equipment and services ready for occupation by business recovery teams at short notice

3 Abbreviations

BCM business continuity management

BCP business continuity plan

BIA business impact analysis

CMP crisis management plan

E2E end-to-end

ITDR information technology disaster recovery

JIT just-in-time

KPI key performance indicator

LBC level of business continuity

MCA mission critical activity

MIS management information system

RA risk assessment

RACI responsible/accountable/consulted/informed

RPO recovery point objective

RTO recovery time objective

SLA service level agreement

WAR work area recovery

4 Overview

4.1 Principles

The operation of any internal activities or outsourcing of products, services, support or data should reflect the following good practice principles and standards.

— BCM is an integral part of corporate governance but should be undertaken because it adds value rather than because of governance or regulatory considerations.

— BCM should be treated as a management-owned and -driven process.

— BCM activities should match, focus upon and directly support the business strategy and goals of an organization.

— BCM should provide resilience within an organization to protect and optimize product and service availability.

— As a value based management process BCM should optimize cost efficiencies.

— An organization and its component parts should be accountable and responsible (see Annex A) for maintaining an effective, up-to-date and fit-for-purpose (see Annex B) BCM competence and capability.

— The component parts of an organization should be responsible for and manage their own business risk (i.e. business ownership of business risk). The management of this business risk should be based upon the individual risk appetite of that organizational area and the risk appetite of the organization as a whole.

— An organization and its component parts should recognize and acknowledge that reputation, brand image, market share and shareholder value risk cannot be transferred or removed by internal sourcing and/or outsourcing.

— An organization's change management process should consider the implications of any change (e.g. new business initiatives, operations, acquisitions, mergers, products, services and organizational infrastructure projects) to BCM.

— All BCM strategies, plans and solutions should be based upon an organization's MCAs identified by a BIA.

— All BIAs and RAs should be focused on an organization's products and services in an end-to-end production context.

— An agreed organization policy, strategy, framework and exercising guidelines for BCM and crisis management should be published and distributed.

— An organization and its component parts should implement and maintain a robust exercising, rehearsal and testing programme to ensure its BCM and crisis management capability is effective, up-to-date and fit-for-purpose.

4.2 BCM lifecycle (model and components)

The BCM lifecycle is a continuous cyclical process (see Figure 3).

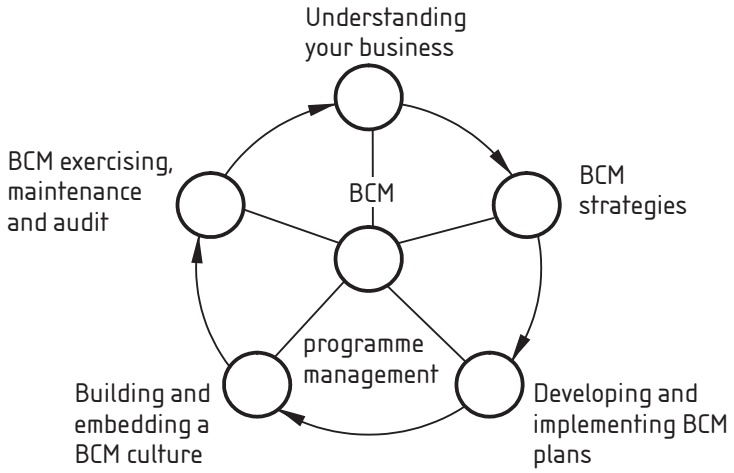

Figure 3 — The BCM lifecycle[5]

5 BCM programme management

5.1 Overview

To be effective BCM should:

— be a business-as-usual management process driven from the top of the organization;

— be fully endorsed and actively promoted by the board or the executive committee;

— have a member of the board or executive committee assigned overall accountability for the effectiveness of the organization's BCM competence and capability (to ensure the BCM programme is given the correct level of importance within the organization, and therefore a greater chance of effective implementation);

— be managed at both operational and organizational levels.

A number of professional BCM practitioners and staff from other management disciplines and departments may be required to support and manage the BCM programme. The quantity of resource required will be dependent upon the size and diversity of the organization, and may be managed using reporting lines and a virtual management structure.

[5] Adapted from Smith, 2002 [1]

It is critical at the genesis of the organization's BCM programme to design and plan to fully integrate the BCM management process and structure into the organizations processes and procedures, and thereby assure the elements identified and described in the BCM life-cycle. This process needs to include the early appointment of clearly defined and documented roles, accountabilities, responsibilities and authorities within the BCM programme. It should ensure:

— these roles, accountabilities, responsibilities and authorities are clearly understood and discharged to people at the right level within the organization, who are empowered to "make things happen";

— that the BCM process is consistent throughout the organization;

— that BCM is recognized as a mainstream management discipline by all executives, managers and staff of the organization, and it is carried out because it adds value;

— that BCM is promoted, communicated and explained to the people involved in the process so that the objectives and requirements are clearly understood and individuals know their responsibilities.

5.2 Management

5.2.1 *General*

In order to effectively measure, control, audit and/or assure the BCM programme, a clearly outlined and documented management process is needed. Roles, accountabilities, responsibilities and authorities should all be clearly defined within the BCM programme and throughout the organization. This can be done by using assigning each role or function a RACI (responsible/accountable/consulted/informed) rating (see Annex A). This will ensure that the programme retains focus and that all participants remain interested and keen to contribute.

5.2.2 *Purpose/objectives*

The purpose of the BCM programme management process is to provide ongoing management, coordination and governance to ensure that all the BCM activities are conducted and implemented in an agreed manner that achieves the organization's BCM and crisis management objectives set out in the BCM policy and business requirements defined through the BIA.

5.2.3 *Outcomes*

The outcomes of BCM programme management should include:

— overall management and assurance of the organization's BCM programme so that it is effective, efficient and fit-for-purpose (see Annex B);

— integration of the management process with the organization's BCM programme and lifecycle;

— awareness at management level that BCM is part of management accountability (i.e. ownership and accountability of BCM should remain firmly within the business line and cannot be outsourced, delegated or off-set);

— the robust and ongoing challenge and review of the organization's BCM risk profile and appetite;

— assurance that BCM is undertaken and based on value-based management principles;

— a management information system (MIS) that provides details of the current state of the organization's BCM programme, incorporates a BCM risk management framework and includes a register of risks or issues, actions, etc.;

— focusing BCM upon the organization's MCAs at a product and service level;

— ensuring that the BCM programme looks at the whole of each MCA, end-to-end, rather than looking at individual elements independently;

— assurance that all the suppliers (internal and external) of services or products on which the MCAs depend are assessed to ensure they have appropriate business continuity arrangements to meet the organization's BCM requirements (RTOs, RPOs and level of business continuity [LBC]);

— optimization of BCM cost efficiencies, e.g. use of BCM information elsewhere within the organization and streamlining operational activities;

— optimization of business processes, product and service resilience and availability;

— assurance that the organization's BCM policy, strategies and operational framework are up-to-date and fit-for-purpose;

— assurance that all new projects are not "signed-off" without a BIA, risk assessment and BCM strategy being in place;

— the following, agreed and signed-off by the organization's executive or senior management:

a) a clearly defined and documented BCM management programme;

b) BCM assurance reports at a predetermined frequency;

c) a clearly defined and documented BCM policy (see 5.3), principles, strategy and set of standards;

d) an annual BCM review;

e) a dedicated BCM budget, including other resource management requirements.

5.3 Policy

5.3.1 *General*

The BCM policy provides the foundation for BCM capability, development and implementation. It should be a clearly defined and documented statement by the organization's executives or senior management outlining the level of importance and value that the organization places on BCM.

5.3.2 *Purpose/objectives*

Formal BCM policy is to provide clearly defined and documented guidance as to how BCM should operate (i.e. its scope, objectives, purpose, aims, review period, commitments, responsibilities, organization, etc.).

5.3.3 *Outcomes*

The outcomes from a BCM policy should include:

— a clearly defined, documented and approved set of BCM principles, guidelines and minimum standards, strategies and operational framework;

— a clearly defined, documented and approved process for the management and assurance of the organization's BCM programme;

— the means whereby the organization and its executive or senior management can discharge its governance and other accountabilities and responsibilities.

5.4 BCM assurance

5.4.1 *General*

A fundamental element of a BCM programme is the need to continually monitor, evaluate and assure its performance. Performance is usually assessed in accordance with key performance indicators (KPIs), but within the context of BCM assurance, performance is measured against the defined outputs specified throughout the stages of the BCM lifecycle.

In order to monitor, evaluate and assure the performance of the BCM programme, procedures (involving defined tasks and checks) need to be put into place to ensure that the programme is meeting the KPIs. Annex B includes a broad set of evaluation criteria against which to measure and verify the intended outcomes.

It is important to assure the completeness of the whole BCM programme rather than just the individual components and stages, (e.g. plans and procedures), to verify that all MCA processes can be recovered to the level required to meet the business requirements.

5.4.2 *Purpose/objectives*

The purpose of BCM assurance is to provide effective and efficient performance monitoring and management to ensure the integrity of the organization's BCM policy, principles and programme.

5.4.3 *Outcomes*

The outcomes of a BCM assurance process should include:

— a clearly defined and documented list of KPIs (objectives, targets and standards) against which to measure the performance of BCM;

— a defined means for monitoring evaluation and review of these KPIs;

— defined means (process or system) by which to determine the level of compliance with the organization's BCM KPIs;

— a level of assurance that the overall management of the organization's BCM programme is effective, efficient and fit-for-purpose, based on achievement of the KPIs and using the evaluation criteria in Annex B as an assessment benchmark;

— the following (clearly defined and documented, and approved and signed-off by the organization's executive or senior management):

a) KPI assurance reports;

b) prioritized remedial action plan(s) to implement the agreed recommendations within the assurance report;

c) a monitoring programme to ensure that remedial action plans are implemented within an agreed timescale.

6 Understanding your business

6.1 Overview

To establish the critical elements for a holistic BCM programme, five basic questions should be asked. These will define the organization's *raison d'être* (its key strategic aims, values and activities) and enable an organization to establish its MCAs.

1. What are the key business objectives?
2. What outputs or deliverables (i.e. products or services) are required in order to meet these business objectives?
3. When do the business objectives need to be achieved?
4. Who needs to be involved (both internally and externally) to achieve the business objectives?
5. How are the business objectives going to be achieved?

Identification of MCAs is essential to enable BCM to aid the achievement of the business objectives. Identification of the dependencies, both internal and external, that either support or provide input to these MCAs also need to be defined, as do any single points of failure (see Figure 4). Dependencies that may support or provide MCAs include:

- human resources;
- suppliers (internal or external service providers);
- customers or clients;
- facilities;
- functions;
- processes;
- materials;
- technology;
- telecommunications;
- data (all formats and media).

To summarize, the key to understanding a business is founded upon identifying:

- MCAs;
- internal and external dependencies for the MCAs;
- single points of failure of the MCAs;
- internal and external influences that may impact upon MCAs.

There are two means by which this understanding can be achieved and the business requirements can be defined:

1. business impact analysis (BIA);
2. risk assessment (RA).

6.2 Business impact analysis

6.2.1 *General*

The BIA underpins the whole BCM process. It consists of techniques and methodologies that can be used to identify, quantify and qualify the impacts on an organization of a loss of, interruption to or disruption of MCAs or their dependencies. It further identifies the minimum level of resources required to enable an organization to achieve its RTOs, RPOs and LBC for MCAs.

The key to a BIA is the recognition that it needs to be conducted in an E2E business service or product context and not in the context of individual components, processes or functions.

A BIA should be undertaken before consideration is given to setting an organization's risk appetite, as it is the BIA and any subsequent risk assessment that informs the setting of a risk appetite.

6.2.2 *Purpose/objectives*

The purpose of a BIA is to identify the business impacts (in terms of loss, interruption or disruption) if MCAs cannot continue and the acceptable time period in which the MCAs and their dependencies need to be recovered to an agreed level of functionality and operation.

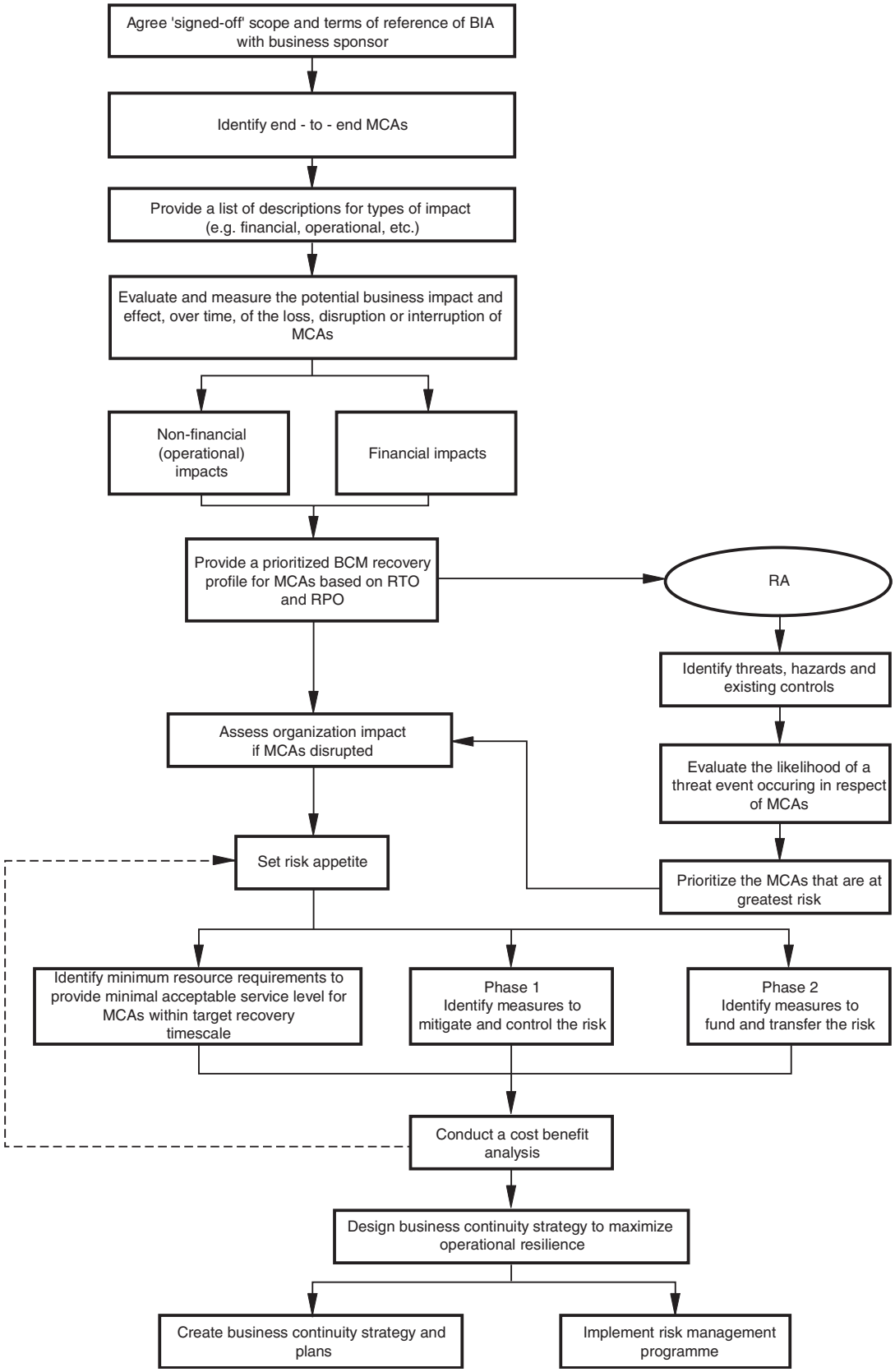

Figure 4 — The BIA and RA process[6]

[6)] Adapted from Rassam , 1999 [3]

6.2.3 *Outcomes*

The outcomes from a BIA should include the identification and documentation of:

— organizational aims, objectives and outputs (services and products);

— E2E MCAs;

— financial and non-financial impacts resulting from the disruption to, interruption to or loss of one or a number of MCAs over various time periods;

— the BCM objectives for each of the organization's MCAs (RTOs, RPOs and LBC);

— the minimum level of resources (phased over time) necessary for an organization to achieve the prioritized recovery of its MCAs to a predefined minimum LBC;

— vital records;

— key customers, clients and stakeholders;

— suppliers (internal and/or outsourced);

— any constraints under which the MCAs need to operate (contractual, legal, regulatory and other);

— the following, signed off by the organization's executive or senior management:

a) a prioritized timeline of activities for the recovery of the organization's MCAs;

b) a schedule of priorities for BCM and investment in business continuity;

c) a BCM resource recovery profile identifying the minimum level of resources necessary, over time, to achieve the prioritized recovery profile of MCAs;

d) multi-level BIA criteria (financial and non-financial).

6.3 Risk assessment

6.3.1 *General*

A major part of BCM is to ensure that the likelihood (frequency and probability) of MCAs being affected by an incident is minimized, and an adequate set of controls is defined, implemented and appropriately managed.

Together with a BIA, an RA provides information to enable a business to determine its risk appetite.

6.3.2 *Purpose/objectives*

The purpose of an RA is to identify, define and evaluate the risks faced by an organization in relation to its MCAs, in order to establish a risk appetite and a plan of action to address (either mitigate or reduce) those risks. The risks may either be internal or external to the organization and should be evaluated in terms of their likelihood (probability or frequency).

6.3.3 *Outcomes*

The outcomes from an RA should include the identification, definition and documentation of:

— the vulnerability and exposure (likelihood of occurrence) of the organization to specific types of incident;

— risk concentration(s), e.g. where a number of MCAs are located within the same building or on the same site;

— a combined BIA and RA to prioritize the focus of BCM and risk controls, enabling the setting of a risk appetite, signed-off by the organization's executive or senior management;

— an assessment of types of risk that pose a threat to the organization;

— the prioritized focus of BCM and risk controls;

— a risk management control strategy and action plan, approved and "signed-off" by the organization's executive or senior management.

7 BCM strategies

7.1 Overview

In the context of BCM, "strategy" concerns the determination and selection of alternative operating methods to be used to maintain the organization's MCAs after an incident, to an acceptable minimum level. Experience and good practice clearly identify that the early provision of an organizational (corporate) BCM strategy will ensure BCM activities are aligned with and support the organization's overall strategy.

There are four basic strategic BCM models:

1. *Active/backup model*
having an "active" operating site with a corresponding backup site for the organization's MCAs (this relies on relocating staff from the active to the backup site where systems and production equipment will need to be available, maintained and up to date);

2. *Active/active (split operations) mode*l
relying upon two or more widely separated (geographically) "active" operational or production sites for MCAs. These sites will inherently back up for one another and share workload. Both sites will have the capacity to handle the full workload if required;

3. *Alternate site model*
having an "active" operating or production site with a corresponding backup site that periodically functions as the primary site;

4. *Contingency model*
having alternative ways of making products or delivering services to cater for the loss of normal operational processes and components (e.g. loss of a system or production equipment may mean reverting to manual methods).

When developing an organization's BCM strategy there are three levels of strategic planning that need to be considered:

— organization (overall) BCM strategy;

— process level BCM strategy;

— resource recovery BCM strategy.

The current trend of developing a "virtual" organization raises a number of specific issues that concern the internal sourcing and outsourcing of MCAs; in particular, the dependencies and single points of failure and the ability to provide alternative sourcing in the event of a catastrophic failure of an MCA provider. This trend, due to the operational and logistical complexity it introduces, reinforces the need for the three levels of strategic planning for BCM.

When developing any level of BCM strategy there are a number of strategic options that should always be considered. These include the following.

a) Doing nothing
A "do nothing" BCM strategy may be acceptable within an organization's risk appetite. Where this is not the case, an organization may still choose to "do nothing" but should recognize that it has increased its risk appetite by taking this approach.

b) Processing transfer
The diversion of the MCA to another organization or alternative part of the host organization. Reciprocal agreements can work in some selected services but due diligence should be taken when establishing this type of arrangement. Such arrangements should be enforceable and subjected to testing via service level agreements (SLAs) or formal contracts.

c) Termination or change
Deciding to change or end a service, product, function or process should be considered as part of the process strategy within the BCM process. This approach is most likely to be seen where a product has a limited lifespan.

d) Insurance
Insurance cover can provide a financial indemnity to an organization following certain defined contingencies. In itself, however, it is not a complete answer, particularly where the incident is not an insured event, or where it escalates into a crisis that threatens that organization's reputation, brand, stakeholder value or market share. These may be its most valuable assets, and under such circumstances a financial settlement alone may not be enough to fully protect the business. A combination of insurance and BCM may be the best overall solution.

e) Loss mitigation
The implementation and management of risk controls and action plans to reduce, minimize or counteract the potential loss.

f) BCM
The improvement of an organization's controls, facilities and preparedness to minimize loss, disruption or interruption to its MCAs to ensure they continue at an acceptable minimum level.

7.2 Organizational BCM strategy

7.2.1 *General*

An organizational (corporate) BCM strategy is key to ensuring resilience and high reliability of the continuance of the organization's MCAs at an acceptable minimum level of business continuity (LBC). Most organizations require BCM to be developed and implemented within the organization design and structure i.e. a "top-down" framework where BCM policy and strategy provides vision and direction. An organizational (corporate) BCM strategy is a living document that encompasses and unifies other BCM related activities.

This type of strategy tends to be developed as an "afterthought" by most organizations when a number of BCM approaches are already in existence and require to be incorporated into a cohesive and integrated BCM framework.

The organizational (corporate) BCM strategy should make reference to specific areas of the process level and resource recovery strategies to enable a smooth transition from one to another, and aid the development of these strategies. This is seen as essential due to the inter-dependencies between the strategies.

7.2.2 *Purpose/objectives*

The purpose of an organizational (corporate) BCM strategy is to provide a clearly defined and documented policy, framework and operational direction to ensure the resilience and continuance of an organization's MCAs to an acceptable minimum LBC.

7.2.3 *Outcomes*

The outcomes from an organization (corporate) BCM strategy should include:

— a clear statement of support for BCM by the organization's executive and senior management;

— the appointment of an executive member of the organization as accountable for BCM within the organization;

— the development of an effective and fit-for-purpose organization (corporate) business continuity plan (BCP);

— defined and agreed risk parameters relating to WAR (where appropriate);

NOTE This can include "syndication ratios", "exclusion zones", the technology refresh period, the time delay for access, etc.

— the identification of key BCM roles, responsibilities and authorities;

— an organization risk appetite statement;

— a BCM policy statement (clearly defined and documented, approved and signed-off by the organization's executive or senior management);

— the provision of fundamental BCM principles, e.g. business risk stays with the business, and how they are to be consistently applied across the organization;

— an operational framework for BCM (clearly defined and documented, approved and signed-off by the organization's executive or senior management);

— assurance that BCM is aligned and supports the overall, strategic aims and business strategies of the organization;

— assurance that BCM will enable preparation for key business, legislative and regulatory changes;

— the definition of the BCM relationship and connection with the security and facilities functions concerning emergency response and evacuation procedures and post-incident salvage and restoration;

— a statement of how the organization will define and manage its MCAs;

— provision for all internally sourced and outsourced MCAs to fall within the scope of the organization's BCM programme;

— a clearly defined and documented management framework and capability to manage and coordinate a BCM incident at an operational or corporate level (approved and signed-off by the organization's executive or senior management);

— the organizational design, financial and other resource profiles and positioning of BCM management within the organization;

— the definition of the BCM relationship, positioning and connection with other risk related functions e.g. operational risk management (ORM);

— the definition of the organization's approach to internal or outsourced third party BCM resource and service specialists, e.g. WAR including syndication ratios, exclusion zones, etc.;

— the approach to be taken in implementing each part of the organization's BCM programme or lifecycle (e.g. BCM maintenance, BCM audit, BCM exercising, BCM assurance, etc);

— an operational crisis management framework (clearly defined and documented, approved and signed-off by the organization's executive or senior management).

7.3 Process level (systemic) BCM strategy

7.3.1 *General*

The process level BCM strategy is a documented framework focused upon the resilience and high reliability of an organization's MCAs from both an organizational and industry perspective.

Every organization should, as a matter of good business practice, define and identify its MCAs in the context of products and services. Within BCM this is identified and documented as part of the BIA. This applies equally to the MCAs of public and private organizations. The global nature of modern businesses, their interlinked dependencies, (automated) processes and high reliance on technology emphasize the catastrophic potential and scale of the business impact if the MCAs fail. This understanding is not only important to BCM but also provides a clear statement of significance to other areas within an organization, e.g. audit, operational risk, information security, and to external organizations, e.g. clients, suppliers and regulators.

Each MCA should have its own BCM strategy, providing a clear statement of how the organization will provide protection and BCM for the MCA.

In determining the process level BCM strategies, they should be clearly linked into the organization (corporate) BCM strategy as they have a direct relationship.

7.3.2 *Purpose/objectives*

The purpose of a process level BCM strategy is to provide a documented framework from which a resource recovery BCM strategy, BCP and a resultant BCM capability can be developed for one or more organizational MCAs.

7.3.3 *Outcomes*

The outcomes from a process level BCM strategy should include:

— an effective and fit-for-purpose BCP for each organization's MCAs;

— agreed principles to be applied when developing resource recovery BCM strategies and BCPs for each MCA;

— the agreed relationship and positioning against the organization's crisis management process;

— links to the organization's crisis management capability;

— assurance that the organization has the capability to define and manage its process level MCAs;

— an organization process MCA risk appetite statement (clearly defined and documented, approved and signed-off by the organization's executive or senior management).

7.4 Resource recovery BCM strategy

7.4.1 *General*

A resource recovery BCM strategy concerns the deployment of appropriate resources as part of a BCP. This type of strategy provides the practical link between the BIA and the development of BCPs.

The resource recovery BCM strategy has a major influence on the BCP for each MCA and is directly linked to the requirements defined from the BIA, e.g. if WAR is necessary, then the strategy should evaluate and document the specific requirements for:

— dedicated work area — scale, location and nature (in-house or third-party);

— syndicated or shared subscription work area — scale, subscription ratio, exclusion zone, etc.;

— reciprocal work area – scale, location, limitations, etc.;

— business response work area — scale, subscription ratio, exclusion zone, etc.;

— mobile recovery solutions — build time, scale, subscription ratio, exclusion zone, etc.

In determining the resource recovery BCM strategy reference should be made to both the process level BCM strategies and the organization (corporate) BCM strategy.

7.4.2 *Purpose/objectives*

The purpose of a resource recovery BCM strategy is to provide a predetermined level of resources within a BCP to enable the implementation of the organization (corporate) BCM strategy and process level BCM strategy.

7.4.3 *Outcomes*

The outcomes of a resource recovery BCM strategy should include:

— the identification of effective and fit-for-purpose resource recovery solutions for the restoration of the minimum level of acceptable functionality of each disrupted, interrupted or lost MCA;

— a framework that clearly identifies and sets out time criticalities, resources and actions to enable the development of a BCP and the capability to achieve the prioritized BCM recovery profile of MCAs, their dependencies and single points of failure within their RTO and RPO.

8 Developing and implementing BCM plans

8.1 Overview

The content and level of detail within each component part of the BCP is dependent upon the nature, scale and complexity of the organization, based upon its risk profile, risk appetite and the environment in which it operates.

In large organizations, it may be more practical to have these components as separate documents and refer to each as an individual plan (this is how this section has been approached). Within smaller organizations (e.g. SMEs), it will most probably be practical to cover each of these component parts within a single document and refer to it as the BCP.

A BCP incorporates a number of key constructs that include:

— solutions;

— time-based objectives (RTOs and RPOs);

— tasks and activities required to achieve time-based objectives;

— procedures or processes;

— information;

— structure;

— teams.

There are two main aspects to delivering effective and fit-for-purpose BCPs and supporting capabilities:

— the formulation of the business continuity solutions, logistics and structure that support the plan;

— the development and documentation of the plan itself.

8.2 Business continuity plan

8.2.1 *General*

The development of a BCP does not signify the end of the BCM process but represents a milestone. A BCP does not provide a BCM competence or capability; it provides the approach to establishing an effective capability. Whilst the plan is of itself important, it is also a representation of the more important BCM planning process and a blueprint to "kick start" the response to a business continuity incident. Consequently, it should be an "action-orientated" document.

The BCP should *omit* the following details as they are not essential to the invocation and operation of the business continuity process:

— BIA;
— RA;
— exercise, rehearsal or testing reports;
— maintenance process;
— audit report;
— other non-essential information.

8.2.2 *Purpose/objectives*

The purpose of a BCP is to provide an effective, fit-for-purpose, predefined and documented framework and process to respond to an incident affecting the organization's MCAs.

8.2.3 *Outcomes*

The outcomes of the BCP should include:

— a clearly defined and documented plan to support the role of the organization's BCM team(s), which is agreed and signed-off by the accountable and/or responsible business owner of the MCAs;
— protection of the organization's reputation and brand image;
— maintenance of public, stakeholder, market and regulatory confidence and trust;
— demonstration of effective and fit-for-purpose BCM and governance to the media, markets, customers, stakeholders and regulators;
— minimization of the impact of a BCM incident on the organization's stakeholders by planning continuity of services, products and resources;
— a process for the management of the business continuity or recovery of MCAs and/or their dependencies within a timeframe (RTO) to an agreed service or production point (RPO);
— the establishment of a clearly predefined and documented BCM response (solutions, timeline of activities and the recovery approach) following a business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed;
— a clearly defined and documented owner of the BCP;
— clearly defined BCP roles, accountability, responsibility and authority.

8.3 Resource recovery and solutions plan

8.3.1 *General*

It is not possible to provide an exhaustive list of potential operational resilience and business continuity resource recovery solutions as this will vary dependent upon the activities performed and the risk appetite of the organization. However, a range of resiliency measures and resource recovery solutions should be considered, prioritized and tiered dependent upon their criticality to the organization as defined by the BIA.

Examples of some resource recovery solutions include:

— insurance;

— WAR;

— remote working;

— displacement.

Where a BCM solution is supported by a contractual commitment it is critical that in addition to the option of renewing the contract, the terms and conditions enable the variation (resilience) of the agreed level of service provision, i.e. upsizing or downsizing together with their associated costs.

8.3.2 *Purpose/objectives*

The purpose of a BCM resource recovery and solutions plan is to provide the key components that support the organization's BCP and deliver the resource recovery BCM strategy.

8.3.3 *Outcomes*

The outcomes from a BCM resource recovery plan should include:

— effective, up-to-date and fit-for-purpose BCM resource recovery solutions for MCAs, which are agreed and "signed-off" by the organization's executive or senior management and/or business unit manager;

— resilient and business-continuity-protected MCAs;

— contracts or SLAs for specialist BCM services, products and resources with either internal or external providers;

— a change control process to ensure that BCM resource recovery solutions for MCAs remain effective, up-to-date and fit-for-purpose;

— assurance that the resource recovery plan can deliver the resource recovery BCM strategy;

— effective and fit-for-purpose procedures to establish the impact an incident has had on an organization's infrastructure or MCAs, i.e. damage assessment.

8.4 Crisis management planning

8.4.1 *General*

The ability to achieve effective crisis management and business continuity during an incident requires strong leadership and coordination between the people responsible, individual site or building crisis management and business crisis management. A further critical aspect of an organization's crisis capability is the competence of the crisis management team.

Failure to put in place an effective and fit-for-purpose crisis management capability and team will expose an organization's brand to unnecessary financial, credit, reputation, regulatory, legal, market and operational risk.

8.4.2 *Purpose/objectives*

The purpose of crisis management is to provide an effective, fit-for-purpose, predefined and documented framework and process to enable an organization to effectively manage specific elements of an incident. This may be of a physical nature (e.g. damage to site), a non-physical nature (e.g. damage to reputation or brand), or a security nature (e.g. kidnap or burglary).

8.4.3 *Outcomes*

The outcomes of crisis management planning should include:

— support for the role of the organization's crisis management team during an incident;

— maintenance of the organization's reputation and brand image;

— maintenance of public, stakeholder, market and regulatory confidence and trust;

— demonstration of effective and fit-for-purpose crisis management and governance to the media, markets, customers, stakeholders and regulators;

— limitation and prevention of the impact of an incident;

— minimization of the impact of crises on the organization's stakeholders by providing continuity of services, products and resources;

— the establishment of a clearly predefined and documented crisis management response following a business crisis - from the initial response to the point at which normal business operations are resumed, which is agreed and signed-off by the organization's executive or senior management;

— a demonstration to stakeholders that the organization has a BCM capability;

— a clearly defined and documented owner for crisis management;

— clearly defined crisis management roles, accountability, responsibility and authority;

— clearly defined and documented CMP that is agreed and signed-off by the organization's executive or senior management;

— clearly defined, effective and fit-for-purpose procedures to deal with the management of incidents (an incident management plan) that include evacuation, liaison with emergency services, internal and external communication, coordination of the response to the incident and escalation.

9 Building and embedding a BCM culture

9.1 Awareness, training and culture

9.1.1 *General*

Creating and embedding a BCM culture within an organization may be a lengthy process. It may encounter a level of resistance that should not be underestimated. Success within an organization is primarily dependent upon the following:

a) BCM becoming an integral part of the organization's strategic and day-to-day management ethos;

b) education, awareness training and participation being used to effect cultural change (merely documenting a BCM strategy and plan represents a narrow and limited method of developing a BCM culture);

c) preparation and delivery of a programme to create corporate awareness and enhance the skills, knowledge and experience required to implement, maintain, manage and execute BCM;

d) a vision statement and the visible proactive support from the organization's executive, senior and middle management;

e) ownership of BCM by the various parts of the organization where operational risk originates and resides (not just within facilities or IT);

f) commitment to maintain and review the organization's BCM policy, strategies, framework, plans and solutions on a regular basis;

g) appreciation and recognition of the importance of BCM to the organization and the role of individuals within it;

h) communication to all external stakeholders and third parties (sourced service providers) upon whom the organization depends, in both normal and incident situations, of the importance of BCM to the organization and their role.

If these approaches are adopted all those associated with the organization should have confidence in its ability to manage during an incident, and the embedding of a successful BCM culture will have begun.

9.1.2 ***Purpose/objectives***

BCM should become an integral part of the organization's strategic and day-to-day business-as-usual operational management as a result of embedding a BCM culture.

9.1.3 ***Outcomes***

The outcomes from a training, awareness and cultural development programme should include:

— a clearly defined and documented BCM vision and policy statement agreed and signed-off by the organization's executive or senior management;

— acceptance and implementation of BCM as a professional management discipline;

— an organizational culture that ensures BCM activities and considerations are integral to the business-as-usual activities throughout the organization at all levels;

— proactive "hands-on" promotion of BCM by the organization's executive, senior and middle management;

— an organizational, managerial and staff BCM competence to execute the organization's BCM strategy;

— an awareness and understanding by the organization's management and staff of the importance of BCM and their roles, accountabilities, responsibilities and authority within it;

— ongoing BCM education and awareness promotion;

— a performance management and appraisal system that explicitly recognizes and reinforces the importance of BCM;

— job descriptions and associated skills that include BCM at all levels within the organization;

— a rewards and recognition system that explicitly recognizes and reinforces the importance of BCM;

— an ongoing programme of BCM training for those directly involved in the implementation, maintenance and execution of the organization's BCM capability;

— a clearly defined and documented management information system to monitor and evaluate the BCM awareness and competency of the organization's staff and managers;

— production of BCM awareness *aide-memoires*.

10 BCM exercising, maintenance and audit

10.1 Exercising

10.1.1 *General*

In the past there has been overemphasis on the exercising of IT systems. This is now recognized as being an overly narrow approach to BCM exercising. The role of people and their skills, knowledge, management and decision-making are the key elements. The need for the rehearsal of peoples' roles is now fully recognized as a critical element within an organization's exercising programme.

Exercising involves the critical testing of BCM strategies and BCPs, rehearsing the roles of team members and staff and testing the organization's systems to demonstrate BCM competence and capability.

No matter how well designed and thought-out a BCM strategy or BCP may be, a series of robust and realistic exercises that test their implementation will identify issues that require attention. An exercise should also be used as an opportunity to measure the quality of planning, competence of individuals and BCM capability.

Positive professional commitment and active participation of staff, managers, directors and executives of the organization who are confident and aware of their BCM strategies and plan, makes BCM exercising more acceptable and enables strengths to be acknowledged and weaknesses to be seen as opportunities for improvement rather than criticism. Exercising is essential in proving that BCM strategies and BCPs are workable. Time and resources spent exercising BCM strategies and BCPs will lead to a fit-for-purpose BCM capability, which is essential at times of crisis and uncertainty.

Good quality exercises rely upon challenging and realistic scenarios, and will clearly identify areas for improvement. An exercising programme should begin simply and escalate gradually (see Figure 5).

The level of resource necessary to support exercising and testing of BCM for automated systems will be determined by the level of business automation deployed within an organization.

Highly automated systems require "high reliability" (and sometimes "high availability") and should be designed to be tested routinely, in the course of normal operations. These tests should be invisible to customers and operations staff alike, and should not create a sense of crisis. Testing such systems may entail switching off items of equipment to monitor for any service effects, or transferring service to another location with no, or very limited, service impact.

Less advanced systems may require significant planning and diverting of production resources to rehearse separate, stand-alone recovery processes and locations, especially if full use of IT disaster recovery and BCP teams are required.

> **NOTE 1** It is important that only the resources available during an actual business continuity incident are used during the exercise.
>
> **NOTE 2** Failure in the testing context is not a negative result. Testing is designed to promote continuous improvement, so a "failure" is considered a positive and beneficial outcome.

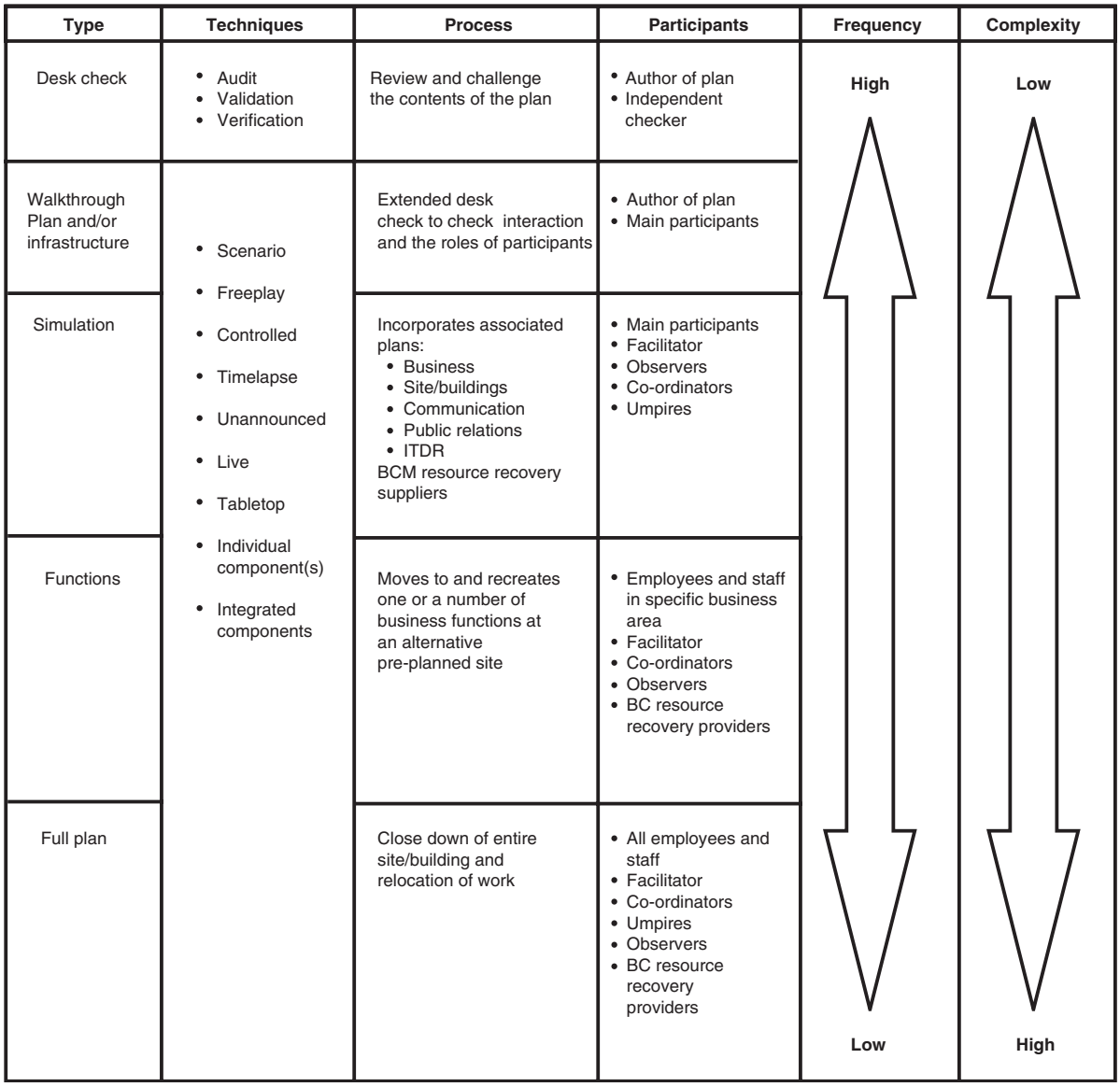

Figure 5 —Exercising types and methods[7]

10.1.2 *Purpose/objectives*

The purpose of exercising is to evaluate and enable the continuous improvement of the organization's BCM competence and capability.

10.1.3 *Outcomes*

The outcomes of the BCM exercising process should include:

— a demonstrable business continuity and crisis management competence and capability;

— verification that the BCP and BCM strategies are workable, effective, up-to-date and fit-for-purpose and will enable the management, control and coordination of a BCM incident at a strategic, tactical and operational level;

— the training or awareness of individuals involved in using the BCM plan(s);

— the rehearsal of roles, leading to familiarization of team members and staff with their roles, accountability, responsibilities and authority in the operation of the BCM plan(s);

— testing of the technical, logistical, administrative and other operational systems of the BCM plan(s);

[7] Adapted from Smith, 2002 [1]

— testing of BCM organization and infrastructure (including command centres, work areas, technology and telecommunications resource recovery, availability and relocation of staff);

— verification that the BCP incorporates all organizational MCAs and their dependencies and priorities;

— the provision of a mechanism to reinforce business continuity and crisis management maintenance and auditing;

— documentation of exercise results for major customers, auditors, insurers, regulators and others;

— increased awareness of emergency procedures;

— increased awareness of the significance of BCM;

— identification of shortcomings and required improvements to the organization's BCM competence and capability;

— the documentation and evaluation of the exercise to provide the foundation of a signed-off and time driven "action point" work schedule to improve the organization's overall BCM competence and capability;

— an amended BCP and BCM strategy that is signed-off by the senior manager of the organization as effective, up-to-date and fit-for-purpose.

10.2 Maintenance

10.2.1 *General*

Most organizations exist in a dynamic environment and are subject to change in people, processes, supplies, market, risk, environment, geography, and business strategy. To ensure that BCM continues to reflect the nature, scale and complexity of the organization it supports, it must be vigorously maintained.

A clearly defined and documented BCM maintenance programme and processes should be established, by ensuring that any changes (internal or external) that impact the organization are reviewed in relation to BCM. This should be agreed and proactively supported by senior management and should involve a wide range of people in both managerial and operational roles from both a business and technical perspective.

Rather than operating a narrow, plan-based BCM model, the BCM of the whole of an organization's business continuity competence and capability should be maintained (e.g. BIA, RA, strategies, etc.), not just the BCP. This critical distinction is frequently overlooked by the organizations that consider BCM to be a BCP.

10.2.2 *Purpose/objectives*

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 to meet the business requirements.

10.2.3 *Outcomes*

The outcomes from the BCM maintenance process should include:

— clearly defined and documented evidence of the proactive management and governance of the organization's business continuity monitoring and maintenance programme;

— details of all changes to the BCM strategy, the BCPs and the organization's processes and systems;

— verification that BCM policy, strategies and plans continue to accurately reflect and be relevant to the organization's business strategy, priorities, aims and objectives;

— validation of the BIA and risk analysis upon which the BCM strategy and BCP is based;

— verification that details within BCM strategies and BCPs are up-to-date, accurate, complete and capable of enabling the appropriate management or coordination of an incident;

— verification that the BCM capability (including strategies and plans) is updated to reflect the lessons learned from exercising and invocation of the plans;

— verification that BCPs follow a logical sequence, format and structure, and conform to industry good practice guidelines and standards;

— verification that effective change (version) control processes or procedures are in place;

— verify and validate that the organization's crisis management competence and capability will enable the management or coordination of an incident at an operational, tactical or strategic (corporate) level;

— verify that key people who will implement the BCM strategy and plans remain in place, maintain a clear understanding of their roles and responsibilities and are familiar with the BCM strategy(ies) and plans;

— identification and documentation of the date of the last and next BCM maintenance together with the person assigned to complete the task;

— the following, clearly defined, documented, and signed-off by the organization's executive or senior management:

a) BCM monitoring and maintenance programme;

b) maintenance report (including recommendations);

c) BCM maintenance report action plan;

d) due diligence reports to the effect that the BCM competence and capability of suppliers (internal or outsourced providers) of MCAs, their dependencies, and recovery suppliers is effective, up-to-date and fit-for-purpose (as defined in contractual terms and conditions or SLAs);

e) effective, up-to-date and fit-for-purpose BCPs, crisis management strategies and solutions concerning the organization's MCAs.

10.3 Audit

10.3.1 *General*

The BCM audit process plays a key role in ensuring that an organization has a robust, effective and fit-for-purpose BCM competence and capability. It has five key functions:

1. to independently verify compliance with the organization's BCM policy, strategies, framework and good practice guidelines or standards adopted by the organization;
2. to independently review the organization's BCM solutions;
3. to independently verify and validate the organization's BCP and crisis management procedures;
4. to independently verify and validate that key exercising and maintenance activities are taking place, in line with the relevant programmes, processes and the organization's BCM framework;
5. to highlight key material deficiencies and issues and ensure their resolution.

The organization's policy concerning the frequency and triggers for the auditing of BCM should be clearly defined and documented within the organization's audit policy (see Annex C).

The BCM audit, like BCM planning, implementation and maintenance, is concerned with a complex process and requires interaction with a wide range of managerial and operational roles from both a business and technical perspective. The following key considerations should be applied to it.

a) The role and perspective of the auditor and audit function is one of impartial review against defined standards. Whilst the auditor may be fully aware of and may identify the reasons for BCM shortcomings and organizational difficulties, the auditor should clearly identify the BCM competence and capability gaps.

b) An integral part of the audit is to provide remedial recommendations.

c) Each stage of the BCM life-cycle may require a different audit approach. The audit approach is solely dependent upon the maturity of each stage of the BCM life-cycle.

d) A proactive audit process should be seen as an enabling process to achieve a particular management objective.

e) The audit process can be undertaken by an organization's internal audit function, an external auditor, or external professional BCM practitioner. The scope of the audit should be material to the organization, clearly defined, documented and agreed in partnership with the relevant auditee and senior management. Where auditors do not have the requisite professional level of BCM knowledge, expertise and experience, they should employ the assistance of a professional BCM practitioner.

10.3.2 ***Purpose/objectives***

The purpose of a BCM audit is to scrutinize an organization's existing BCM competence and capability, verify it against predefined standards (e.g. the assessment criteria in Annex B) and criteria, and deliver an audit report detailing the findings, conclusions and recommendations.

10.3.3 ***Outcomes***

The outcomes from a BCM audit should include verification that:

— issues of operational resilience, e.g. MCAs and their dependencies, have been identified and included in the organization's BCM strategies and plans;

— the organization's BCM policy, strategies, framework and plans continue to reflect accurately and be relevant to the organization's priorities and requirements and reflect industry good practice guidelines and standards;

— the organization's BCM competence and its BCM capability are effective and fit-for-purpose and will enable management, command, control and coordination of a BCM incident;

— the organization's BCM solutions are effective, up-to-date and fit-for-purpose;

— the organization's BCM exercising programme is being effectively implemented;

— the organization's BCM maintenance programme is being effectively implemented;

— BCM strategies and BCPs are updated to reflect the lessons learned from the BCM maintenance programme;

— a documented change control process or procedure is in place and operating effectively;

— a clearly defined and documented audit contract and plan (statement of work and scope) is agreed and signed off by the senior management of the auditee;

— an independent audit opinion report is agreed and signed-off by the senior management of the auditee;

— a clearly defined, prioritized and documented remedial action plan(s) is agreed and signed-off by the senior management of the auditee to implement the agreed recommendations of the independent audit report;

— a clearly defined and documented monitoring programme is agreed and signed-off by the senior management of the auditee to ensure that remedial action plans are implemented within the agreed timescale.

Annex A (informative)
Participants in the BCM cycle

The roles and functions listed in Table A.1 (not restrictive or exhaustive) are examples of the types of roles and functions that may be responsible or accountable or should be either consulted or informed during each stage of the BCM process.

Complete a form such as the one shown in Table A.1 for each stage of the BCM lifecycle. Consider, for each stage, which people or functions should be involved. Designate the type of involvement required from each role/function in the list (RACI).

NOTE Some roles or functions on the list may not need to participate at all.

Table A.1 —RACI participants in the BCM cycle

Stage of the BCM process:				
Role or function	**Responsible R**	**Accountable A**	**Consulted C**	**Informed I**
Executive or senior management				
Executive or senior business manager accountable for BCM within the organization				
Business continuity manager				
Operational middle management				
Operational supervisors and staff				
Professional BCM practitioner				
Emergency services				
Local authority emergency planning				
Health and safety				
Risk management (all types)				
Training and development				
Human resources				
Audit/assurance				
Regulatory				
Legal				
Finance				
Telecommunications				
Technology				
Facilities/property management				
Suppliers of specialist BCM resources and services (internal or outsourced providers)				
Insurance				
Security				
Communications and public relations				
Unions and staff associations				
Commercial services management				
Relationship management				
Subject experts (where appropriate)				
Suppliers of business services or products (internal or outsourced providers)				

Annex B (informative)
BCM evaluation criteria

B.1 General

The evaluation criteria described in **B.2** to **B.7** are based on a set of core questions that reflect the six stages of the BCM lifecycle. They can be used either as part of a self assessment process or by an auditor as part of a formal audit.

The evaluation criteria have been designed to facilitate a multi-stage assessment of an organization's business continuity and crisis management competence and capability, and can be used as benchmark comparators.

All questions are of equal value and weighting.

> **NOTE** The questions themselves do not provide a quality assurance audit. Quality assurance auditing requires the assistance of a professional BCM practitioner, and may involve a further, rigorous quality assurance review, verification and validation (accreditation) process.

The aim of the evaluation process is to:

— provide a consistent BCM good practice benchmark;

— enable and inform the identification of an organization's BCM KPIs;

— identify gaps in an organization's BCM competence and capability;

— demonstrate and provide evidence that the organization is discharging its legal, regulatory and corporate governance accountability and responsibilities.

B.2 BCM programme management

B.2.1 *Management*

— Does the organization have a clearly defined, documented and approved management process to manage its BCM programme?

— Does the organization use PAS 56 as an integral part of its BCM programme?

— Does the organization's BCM programme management process achieve the outcomes of BCM programme management as set out in **5.2.3**?

— Does the organization's BCM programme clearly identify and comply with current regulatory, legal and the organization's BCM policy and principle requirements?

— Are professionally qualified BCM practitioners involved in the implementation of the organization's BCM programme?

— Have the overall organizational accountability and responsibilities for the management of the organization's BCM programme been clearly defined and documented?

— Has the organization successfully demonstrated its BCM (including crisis management) competence and capability via exercising, rehearsal and testing or invocation?

— Does the organization's BCM programme incorporate the allocation of dedicated resources and finance as a part of the annual budget development and management process?

— Does the management of the organization's BCM programme focus upon the organization's MCAs at a product and service level?

— Is the management of the organization's BCM programme based upon an E2E approach in the context of product and service delivery?

— Does the management of the organization's BCM programme provide assurance that suppliers (internal and/or outsourced providers) of the organization's MCAs have an effective, up-to-date and fit-for-purpose BCM capability?

— Does the organization have a Management Information System (MIS) to monitor and provide regular reports concerning the status of BCM within the organization?

B.2.2 ***BCM policy***

— Does the organization have a clearly defined, documented and approved BCM policy?

— Does the organization's BCM policy include the BCM principles set out in **4.1**?

— Does organization's BCM policy achieve the outcomes of a BCM policy as set out in **5.3.3**?

— Does the organization's BCM policy enable corporate governance, the discharge of its responsibilities and satisfaction of its legal and regulatory obligations?

— Does the organization's BCM policy provide for a clearly defined, documented and approved set of BCM guidelines and minimum standards?

— Does the organization's BCM policy provide for a clearly defined, documented and approved independent audit process including frequency and triggers of the organization's BCM capability (not just plans)?

— Does the organization's BCM policy provide for the verification and validation of the effectiveness and fit-for-purpose BCM capability of the suppliers (internal and/or outsourced providers) of its MCAs?

B.2.3 ***BCM assurance***

— Does the organization have a clearly defined, documented and approved BCM assurance management process and frequency (cycle)?

— Does the organization's BCM assurance process achieve the outcomes of a BCM assurance process as set out in **5.4.3**?

— Does the organization have a set of clearly defined, documented and approved KPIs (objectives, targets and standards) for BCM?

— Does the organization have a clearly defined and documented monitoring, evaluation and review process for its BCM KPIs?

— Does the organization's BCM assurance process provide clearly defined, documented and approved management information assurance reports?

— Does the organization's BCM assurance process provide clearly defined, approved, prioritized and documented remedial action plan(s) to implement the agreed recommendations of the assurance report?

B.3 Understanding your business

B.3.1 ***Business impact analysis***

— Has the organization adopted a clearly defined and documented standard BIA process?

— Does the organization's BIA process achieve the outcomes of a BIA as set out in **6.2.3**?

— Was the current BIA completed within the last 12 months?

— Was the current BIA conducted in an E2E business service or product context?

— Has the organization clearly identified, defined and documented its MCAs (including outsourcing of products and services)?

— Has the organization clearly defined and documented the RTO, RPO and LBC for its MCAs (products and services)?

— Does the BIA identify resource recovery requirements?

— Does the organization have a process to ensure that a BIA is carried out as a part of all project and change management including new developments of (and major changes to) IT systems, services and their sourcing?

B.3.2 ***Risk assessment***

— Does the organization have a clearly defined, documented and approved risk management strategy?

— Does the organization's risk assessment process achieve the outcomes of a risk assessment as set out in **6.3.3**?

— Does the organization have a clearly defined, documented and approved standard process to carry out an operational risk assessment?

— Does the organization have a clearly defined and documented process to ensure the approved risk methodology, tools, techniques and criteria are consistently applied?

— Does the organization have a clearly defined, documented and approved organization risk appetite benchmark, including the acceptance of residual risk?

— Has a risk assessment been completed within the last 12 months in respect of the organization's MCAs?

— Has the organization identified its own organizational and industry systemic risks?

— Has the organization identified its areas of high risk concentration e.g. one building/site with several MCAs?

— Has the organization introduced risk management controls (an action plan) to eliminate, mitigate, reduce, transfer the effects of identified key threats, vulnerabilities, exposures or liabilities to MCAs?

B.4 BCM strategies

B.4.1 ***Organization BCM strategy***

— Does the organization have a clearly defined, documented and approved organization BCM strategy?

— Does the organization BCM strategy achieve the outcomes of an organization BCM strategy as set out in **7.2.3**?

— Is the organization's BCM strategy clearly linked to, aligned to and supporting the overall strategic aims and business strategies or plan of the organization?

— Does the organization have a clearly defined, documented and approved BCM framework?

— Has the organization identified key roles, responsibilities and authorities within its organization BCM strategy?

B.4.2 ***Process level (systemic) BCM strategy***

— Does the organization have a clearly defined, documented and approved process level BCM strategy?

— Does the organization's process level BCM strategy achieve the outcomes of a process level BCM strategy as set out in **7.3.3**?

— Has the organization identified key roles, accountabilities, responsibilities and authorities within its process level BCM strategy?

— Has the selected process level BCM strategy(ies) been fully evaluated to ensure it is fit-for-purpose and capable of working within the required timescales?

B.4.3 ***Resource recovery BCM strategy***

— Does the organization have a clearly defined, documented and approved resource recovery BCM strategy?

— Does the resource recovery BCM strategy incorporate the resource recovery requirement from the BIA?

— Does the organization's resource recovery BCM strategy achieve the outcomes of a resource recovery BCM strategy as set out in **7.4.3**?

— Have the key roles, accountabilities, responsibilities and authorities within the resource recovery BCM strategy been clearly defined and documented?

— Has the resource recovery strategy been fully evaluated to ensure it is fit-for-purpose and capable of working within the required timescales?

— Have both technical (e.g. IT, telecommunications, WAR, specialist services) and non-technical (e.g. people and equipment) issues been considered within the resource recovery BCM strategy?

— Has the internal sourcing and outsourcing of products and services been included within the resource recovery BCM strategy?

B.5 Developing and implementing BCM plans

B.5.1 ***Business continuity plan***

B.5.1.1 *General*

— Does the organization have a clearly defined, up-to-date, fit-for-purpose and approved BCP(s) for all its MCAs?

— Does the BCP reflect the most up-to-date BIA, business impact resource recovery requirements and RA?

— Does the BCP establish a clearly predefined BCM response (solutions, resumption and recovery) following a business disruption, interruption or loss of the organization's MCAs from the initial response to the point at which normal business operations are resumed?

B.5.1.2 *BCM planning*

— Does the organization have a clearly defined, documented and approved BCM planning process framework?

— Does the organization's BCM planning process achieve the outcomes of the BCM planning process set out in **8.2.3**?

— Is the organization's BCM planning process primarily concerned with its MCAs?

— Is the planning process coordinated with the organization's service or product sourcing (outsourcing and internal sourcing) providers?

— Is the organization's BCM planning process integrated and coordinated with other parts of the organization e.g. geographically (departments, sites, etc.)?

— Are BCP templates, frameworks, sample plans or minimum standards available for reference and to provide a standardized BCM planning approach?

B.5.1.3 *Emergency BCM response procedures*

— Does the BCP provide a clearly defined, up-to-date and fit-for-purpose BCM emergency response?

— Does the BCP provide a clearly defined process to ensure there are links to other organizations e.g. emergency services, or suppliers that may be involved in the recovery and restoration process?

B.5.1.4 *Notification, invocation and escalation*

— Does the BCP have a clearly defined and structured up-to-date and fit-for-purpose BCM notification, invocation and escalation process?

— Has the effective capability of the notification, invocation and escalation process been demonstrated and proven via exercising and/or invocation?

B.5.1.5 *Roles, accountability, responsibility and authority*

— Is the role of organization's executive or senior management during a BCM incident clearly defined, approved and documented?

— Does the BCP clearly define the BCM roles and their accountability, responsibility and authority?

— Has each BCP role been assigned to a principal and an alternate individual, should the principal be incapacitated or otherwise unavailable?

B.5.1.6 *Key supporting information*

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

B.5.1.7 *People issues*

— Does the BCP contain either mandatory instructions, advice, process, procedure or guidelines concerning casualties and fatalities?

— Does the BCP contain mandatory instructions, advice, process, procedure or guidelines concerning confidential staff counselling and staff welfare, e.g. consideration of personal belongings, travel and relocation issues?

B.5.1.8 *Communication*

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

B.5.1.9 *Documentation, forms and checklists*

— Does the BCP have an up-to-date task list that clearly identifies both mandatory and discretionary tasks together with the individuals accountable or responsible for their completion within an allocated timeframe?

— Does the BCP provide an auditable process for tracking and recording the completion of the BCP task list after the plan has been invoked and any additional on-going tasks?

— Does the BCP provide up-to-date (internal and external) contact lists (e.g. for key and alternate staff, suppliers, stakeholders, etc.)?

— Has a current list of key service providers, suppliers and other third-party sourcing contacts been identified and documented within the BCP?

— Does the BCP provide a situation management and decision log template?

B.5.1.10 *External bodies and organizations*

— Has an Emergency Services Liaison Officer been appointed?

— Have statutory/regulatory/official agencies been identified and included in the organization's BCM planning process?

— Does the BCP provide clearly defined coordination procedures for local authorities, service utilities and other relevant public authorities?

B.5.1.11 *Media and public relations*

— Does the BCP provide a clearly defined process for dealing with the media and public relations during a BCM situation?

B.5.2 ***Resource recovery and solutions plan***

B.5.2.1 *General*

— Have the "owners" of the organization's MCAs and dependencies developed and implemented BCM solutions within their BCM strategy or plan to achieve the RTO, RPO and LBC of their MCAs?

— Does the resource recovery and solutions plan achieve the resource recovery and solutions plan outcomes as set out in **8.3.3**?

B.5.2.2 *Insurance*

— Are all BCM insurance policies and their coverage limits reviewed regularly for adequacy and cost benefit?

B.5.2.3 *People*

— Does the BCP clearly identify key members of staff (according to their skills, knowledge, organizational role and experience) and a process or strategy to ensure their availability?

B.5.2.4 *Work area recovery (WAR)*

— Has a WAR strategy for MCAs and their support activities been developed and documented within the BCP?

— Is the WAR site located at least 800 metres (based on a large vehicle bomb) from the site of the incident, so as not to be affected by the same incident?

— Is the level of specialist service support required to enable the use of the WAR site and its services clearly identified within a service contract or SLA?

B.5.2.5 *Information technology*

— Has an information technology resumption and recovery strategy for MCAs and their dependencies been developed and clearly documented within the BCP?

— Does the BCP clearly identify that the technical recovery site is located at least 800 metres (based on a large vehicle bomb) from the site of the incident, so as not to be affected by the same incident?

— Have the business owners of the MCAs and the technical and/or specialist third party service providers successfully tested the resumption and/or recovery of the IT systems?

B.5.2.6 *IT software*

— Does the BCP provide a clear inventory of all IT systems software necessary for the BCM of MCAs to achieve their BCM RTO, RPO and LBC objectives?

— Does the BCP provide clear details of specialist software configuration(s) and a process for its restoration, including licensing arrangements?

— Have arrangements been made to place specialist software in escrow?

— Have the business owners of the MCAs and technical and/or specialist third party service providers successfully tested the resumption and/or recovery of the IT software systems?

B.5.2.7 *Telecommunications*

— Has a telecommunications recovery strategy for MCAs been developed and clearly defined within the BCP?

— Have the business owners of the MCAs and suppliers and/or specialist third party service providers successfully tested the resumption and/or recovery of the telecommunications systems?

B.5.2.8 *Data*

— Does the organization have clearly defined backup procedures for all applications, hardware and data (both electronic and paper, e.g. records, unique records or documents) necessary to support MCAs?

— Does the organization have clearly defined recovery and restoration processes and procedures in place for all data (both electronic and paper , e.g. records, unique records or documents) necessary to support MCAs?

— Have the business owners of the MCAs, technical staff, WAR providers and specialist third-party data storage providers successfully tested the recovery and restoration of vital records (both electronic and paper)necessary to support MCAs?

— Can vital records (both electronic and paper) necessary to support MCAs and their dependencies be recovered simultaneously at more than one WAR site if required?

B.5.2.9 *Equipment*

— Does the BCP provide clear details and a list of equipment e.g. photocopier, manufacturing machinery, etc. needed for MCAs?

B.5.2.10 *BCM service providers*

— Is the level of specialist BCM service required to enable the use of a WAR site or other services clearly identified and documented within the service contract and/or SLA, and a copy placed in the BCP?

— Does the BCP provide clear details and a process for the initiation and progressing of recovery, restoration and salvage service by specialist BCM service suppliers?

B.5.2.11 *Security*

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

B.5.2.12 *Business processes*

— Does the BCP provide clear details and a process for recovering MCA work in progress?

— Does the BCP provide clear details and a process concerning work backlog processing?

— Does the BCP provide clear details and a process for the provision of manual operations and fallback solutions and related activities to achieve MCA RTOs and RPOs wherever gaps exist between IT resumption and/or recovery capabilities and BCM needs?

B.5.2.13 *Change management*

— Does the organization have a clearly defined change control process to ensure BCM requirements and selected BCM solutions are maintained in an up-to-date and fit-for-purpose status?

B.5.2.14 *Sourcing (internal and outsourcing)*

— Does the organization maintain a schedule of its sourced (internal or outsourced) MCAs?

— Does the organization's BCM policy clearly define that an outsourced or internal provider of MCAs should have a verifiable, fit-for-purpose and demonstrated BCM capability?

— Does the organization have a clearly defined due diligence process to verify and validate that outsourced or internal providers of MCAs have a fit-for-purpose and demonstrated BCM capability in respect of each MCA?

— Does the organization have a clearly defined and documented structure to "relationship manage" any sourcing of its MCAs?

— Does the organization have a supplier exit strategy or plan, i.e. the capability to switch the provision of the MCA to another outsourcer or to internal provision, to cover the complete failure of any contract or SLA for each of its sourced MCAs?

— Does the sourcing contract and/or SLA of the organization's sourced MCAs include a right by the organization to audit the BCM capability and resilience of the supplier against predefined and agreed BCM standards (e.g. within RTOs, RPOs and to the minimum LBC)?

— As a part of the organization's due diligence process of the sourcing of its MCAs, does the organization regularly receive certified copies of the supplier's own internal BCM exercising reports and action plans?

B.5.3 ***Crisis management***

B.5.3.1 *Crisis management planning*

— Does the organization have a clearly defined, documented and approved crisis management framework?

— Are professionally qualified crisis management practitioners involved in the planning process?

B.5.3.2 *Crisis management plans*

— Does the organization have a clearly defined, up-to-date, fit-for-purpose and approved crisis management plan (CMP)?

— Does the organization's CMP achieve the outcomes of a CMP as set out in **8.4.3**?

B.5.3.3 *Emergency procedures*

— Does the CMP clearly set out and document emergency evacuation procedures; other staff and building safety procedures; evacuation and assembly points for different types of incident (e.g. fire or bomb) and their testing programme?

B.5.3.4 *Control and coordination centres*

— Does the CMP provide a clearly defined control and coordination organization structure to manage an incident?

— Has the effective capability of the control and coordination centre(s) been demonstrated and proven via exercising and/or invocation?

B.5.3.5 *Notification, invocation and escalation*

— Does the CMP have a structured up-to-date, fit-for-purpose and approved incident notification, invocation and escalation process?

— Has the effective capability of the notification, invocation and escalation process been demonstrated and proven via exercising and/or invocation?

B.5.3.6 *Roles, accountability, responsibility and authority*

— Is the role of the organization's executive or senior management during an incident clearly defined, agreed and documented?

— Does the CMP clearly define the organization's crisis management roles, accountabilities, responsibilities and authorities?

— Has each CMP role been assigned to a principal and an alternate individual should the principal be incapacitated or otherwise unavailable during an incident?

B.5.3.7 *Key supporting information*

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

B.5.3.8 *People issues*

— Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning casualties and fatalities?

— Does the CMP contain either mandatory instructions, advice, process, procedure or guidelines concerning confidential staff counselling and staff welfare, e.g. consideration of personal belongings, travel and relocation issues?

B.5.3.9 *Communication*

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

B.5.3.10 *Documentation, forms and checklists*

— Does the CMP have an up-to-date task list that clearly identifies both mandatory and discretionary tasks together with the roles accountable or responsible for their completion with an allocated timeframe?

— Does the CMP provide an auditable process for tracking and recording the completion of the CMP task list(s) after the plan has been invoked?

— Does the CMP provide up-to-date (internal and external) contact lists (e.g. for key and alternate staff, suppliers, stakeholders)?

— Does the CMP provide a crisis management and decision log template?

B.5.3.11 *External bodies and organizations*

— Has an individual been clearly identified and appointed to the role of emergency services liaison officer within the CMP?

— Does the CMP provide clearly defined and documented coordination procedures for local authorities, utility services and other relevant public authorities?

B.5.3.12 *Media and public relations*

— Does the CMP contain a clearly defined media and public relations strategy and plan?

— Does the CMP clearly identify and unambiguously describe stakeholders and interest groups?

B.6 Building and embedding a BCM culture

— Does the organization have a clearly defined, published and approved BCM vision and policy statement?

— Does the organization's awareness, training and cultural development programme achieve the outcomes set out in **9.1.3**?

— Have the BCM policy, principles and programme been communicated throughout the organization?

— Does the organization's executive or senior and middle management proactively demonstrate its support and strong commitment to the organization's BCM vision, policy and programme?

— Are the implementation and maintenance of the organization's BCM policy and principles strictly monitored and evaluated?

— Are BCM roles, accountabilities, responsibilities and authorities clearly defined and documented within job descriptions at all levels of the organization?

— Is BCM integrated with the organization's reward and recognition system?

— Is BCM integrated with the organization's performance management and appraisal system?

— Does the organization have clearly defined and documented KPIs for BCM?

— Is BCM an integral part of the organization's change management process?

— Is BCM integral part of the organization's project management process?

— Does the organization have a formal BCM awareness or induction training programme for all new and existing managers and staff?

B.7 Exercising, maintenance and audit

B.7.1 *Exercising*

— Does the organization have a clearly defined, documented and approved BCM exercising cycle and programme?

— Does the organization's BCM exercising programme achieve the outcomes of a BCM exercising programme as set out in **10.1.3**?

— Is a "live" exercise(MCA) run in a "business as usual" context for one week every six months at the WAR location?

— Is the six monthly "live" BCM exercise coordinated, integrated and linked with other organizations' stakeholders and regulators?

— Does the organization have a clearly defined, documented and approved standardized exercise contract that must be approved and signed-off by the exercise sponsor and other participants prior to each scheduled exercise?

— Does the organization's exercising, rehearsal and testing programme provide for various methods, types and techniques of exercising, rehearsal and testing?

— Does the frequency of BCM and crisis management exercising, rehearsal and testing reflect the nature, scale, complexity, culture and operating environment of the organization?

— Does the organization use professionally qualified practitioners to plan and facilitate BCM and crisis management exercises, rehearsals and tests?

— Does the organization provide clearly defined, documented and approved exercising, rehearsal and testing guidelines?

— Does the organization have a clearly defined, documented and approved process to verify that the business continuity competence and capability is being exercised in line with the organization's BCM exercising programme?

— Does the organization have a clearly defined, documented and approved process to provide a standardized post-exercise, rehearsal and/or testing evaluation report?

— Does the organization have a clearly defined and documented post exercise process to provide an approved, prioritized, time-scaled action plan to implement lessons learned, changes and amendments as identified within the recommendations of the post-exercise report?

B.7.2 ***Maintenance***

— Does the organization have a clearly defined, documented and approved BCM maintenance cycle and programme?

— Does organization's BCM maintenance programme achieve the outcomes of a BCM maintenance programme as set out in **10.2.3**?

— Does the organization's BCM maintenance programme cover the whole of the organization's BCM capability and not solely BCP(s)?

— Does the frequency of the BCM management maintenance programme reflect the nature, scale, complexity and culture of the organization including its operating environment, risk profile and risk appetite?

— Does the organization have a clearly defined, documented and approved process for escalating BCM non-compliance issues as highlighted by individuals, exercising reports, assurance report and/or audit findings or situations?

— Does the organization have a clearly defined and documented BCM maintenance process to ensure the BCM competence and capability of sourcing suppliers (internal or outsourced providers) of MCAs is effective and fit-for-purpose (as defined in contractual terms and conditions or SLAs)?

— Does the organization have a clearly defined, documented and approved BCM maintenance process to ensure the BCM competence and capability of suppliers of BCM specialist services (internal or outsourced providers) concerning the organization's MCAs is effective and fit-for-purpose (as defined in contractual terms and conditions or SLAs)?

— Is there a clearly defined, documented and approved process within the BCM and CMP to provide an approved and time-scaled action plan to implement lessons learned, changes and amendments to the organization's BCM and/or crisis management capability as identified within either a BCM or crisis management exercise, audit or assurance report?

— Does the organization's BCM and crisis management maintenance process provide a clearly defined, documented and approved procedure to ensure that all changes to the BCM strategy and/or BCP are reflected in the BCM exercising, training and awareness programmes?

B.7.3 ***Audit***

— Does the organization have a clearly defined, documented and approved BCM audit cycle and programme?

— Does organization's BCM audit process achieve the outcomes of a BCM audit process as set out in **10.3.3**?

— Does the organization's audit policy clearly define the minimum level of frequency and the triggers at which the organization's BCM and crisis management capability should be audited?

— Are the terms of reference and details of a BCM audit clearly defined and documented in the audit contract?

— Does the audit contract clearly identify any external or other professional assistance needed to perform the audit?

— Is a prioritized and signed-off audit opinion report produced after each audit?

— Is a prioritized and signed-off BCM or crisis management action plan to address issues identified during an audit prepared and implemented after each audit, with a specific timescale?

Annex C (informative)
Frequency and triggers

Whilst the various components of a BCM programme should be reviewed on an ongoing basis, the frequency and triggers that determine when they should be reviewed or audited is dependent upon the nature, scale and complexity of the organization, based on its business risk profile, risk appetite and the environment in which it operates.

Good practice indicates that subject to the aforementioned conditions, and following the initial introduction of a BCM programme, a formal review or audit should be carried out, at a minimum, every 12 months unless there are major business changes including:

— redefinition of business strategy or objectives;

— relocation;

— large scale change in staff numbers or office densities;

— initial outsourcing or internal sourcing of MCAs;

— changes to key suppliers (internal and/or outsourced providers);

— process re-design;

— development of new business line(s), product(s) or service(s);

— a merger;

— an acquisition;

— significant changes in the key technology and/or telecommunications systems or networks;

— significant changes in the regulatory or legal environments;

— a BCM incident;

— changes in BCM strategy and/or scope;

— developments in BCM solutions.

Bibliography

[1] SMITH, D. J., ed. *Business continuity management: Good practice guidelines*. Worcester: The Business Continuity Institute, 2002.

[2] SMITH, D.J. A recipe for chaos. *Risk management bulletin*. 2001, **6** (1), 9–14.

[3] RASSAM, C. A matter of control. *International journal of business continuity management*. February 1999, 58–59.
See www.thebci.org

AS/NZS 4360:1999: *Risk management*.

AUSTRALIAN NATIONAL AUDIT OFFICE [Australian Federal Government, Canberra]. *Business continuity management — Keeping the wheels in motion: a guide to effective control*. Canberra [NSW]: Australian National Audit Office, 2000. ISBN 0-644-390182-2.

BIRD, L. Why business continuity is a must have for smaller companies. *International journal of business continuity management*. 2001, **2** (1), 8–11.
See www.thebci.org

BLAND, M. *Communicating out of a crisis*. Basingstoke: Macmillan Publishers Ltd, 1998. ISBN 0-333-72097-0.

EMERGENCY MANAGEMENT AUSTRALIA. *Non-stop service: continuity management guidelines for public sector agencies*. Canberra: 1997.

FEDERAL RESERVE BANK. *Summary of "lessons learned" and implications for business continuity*. New York: 2002.
See www.federalreserve.gov/boarddocs/staffreports/200202/DiscussionNote.pdf

FERGUSON, R.W. *A supervisory perspective on disaster recovery and business continuity*. Remarks by Mr Roger W Ferguson, Jr, Vice Chairman of the Board of Governors of the US Federal Reserve System, before the Institute of International Bankers, Washington, D.C., 4 March 2002.
See www.bis.org/review/r020308c.pdf

FINANCIAL SERVICES AUTHORITY. *FSA working paper on business continuity management*. London: 29 April 2002.
See www.financialsectorcontinuity.gov.uk/home/pdf/fsa_working_paper_on_bcm.pdf

HILES, A. and P. BARNES, eds. *The definitive handbook of business continuity management*. John Wiley & Sons, 2001. ISBN 0-471-48559-4.

HONOUR, D. (2001) Heeding the lessons of 9/11. *International journal of business continuity management*. 2001, **2** (1), 13–17.
See www.thebci.org

INSTITUTE OF DIRECTORS. *Business continuity: helping directors build a strategy for a secure future*. London: Institute of Directors, 2000. ISBN 0-7494-3561-3.

JONES, M.E. and G. SUTHERLAND. *Implementing Turnbull: A boardroom briefing*. London: Centre for Business Performance, The Institute of Chartered Accountants in England and Wales, 1999.

KAYE, D. *Risk management*. Study course 655. London: Chartered Insurance Institute, Publishing Division, 2001.

KEELING, C. *Business continuity management*. London: ICAEW Faculty of Information Technology, 2002.

KNIGHT, R.F. and D.J. PRETTY. *The impact of catastrophes on shareholder value*. Oxford: Templeton College, Oxford Executive Research Briefings, 2000.

LAYE, J. *Avoiding disasters: how to keep your business going when catastrophe strikes*. John Wiley & Sons, 2002. ISBN 0-471-22915-6.

LEATHER, G. Wider than IT. *Continuity*. 2001, **5** (1), 4–5.
See www.thebci.org

LONDON EMERGENCY SERVICES LIAISON PANEL. *Major incident procedure manual*. 5th ed. London: Metropolitan Police Service, 1999.

MITROFF, I.I. and C.M. PEARSON. *Crisis management: a diagnostic guide for improving your organization's crisis preparedness*. San Francisco: Jossey-Bass, 1993. ISBN 1-555-42563-1. Out of print.

POWER, P. *Management action notes: Business continuity management — preventing chaos in a crisis*. London: Department of Trade and Industry, 1999.

SHARP, J. Business continuity management as a board strategy. *Risk management bulletin*. 2001, **6** (1), 15–17.
See www.thebci.org

SIMMS, J. Tick box management of BCPs. *Continuity*. 2001, **5** (2), 10–11.
See www.thebci.org

SMALLMAN, C. Risk and organizational behaviour. *Disaster prevention and management*. 1996, **5** (2), 12–26.

SMITH, D.J. Business continuity and crisis management. *Management quarterly*. 2003, **18**, 27–33.
See www.thebci.org

SWARTZ, E., D. ELLIOTT, and B. HERBANE. *Business continuity management: a crisis management approach*. London: Routledge, 2002. ISBN 0-415-20492-5.

TEHRANI, N. Dealing with disasters: the people issues. *Continuity*. 1999, **3** (3),10–11.
See www.thebci.org

THE BUSINESS CONTINUITY INSTITUTE. *Getting started*. Worcester: 2001.

TOFT, B. and S. REYNOLDS. *Learning from disasters: a management approach*. 2nd ed. Guildford: Perpetuity Press, 1997. ISBN 1-899-28705-1.

TOIGO, J.W. *Disaster recovery planning: for computers and communication resources*. John Wiley & Sons, 1996. ISBN 0-471-12175-4.

TURNER, B.A. and N.F. PIDGEON. *Man-made disasters*. 2nd ed. Oxford: Butterworth-Heinemann, 1997. ISBN: 0-750-62087-0. Out of print.

UNITED KINGDOM . Civil Contingencies Secretariat, The Cabinet Office. *Business as usual: maximising business resilience to terrorist bombings*. London: HMSO, 2001.
See www.ukresilience.info/contingencies/business/business.pdf

UNITED KINGDOM. Central Computer and Telecommunications Agency — the Government Centre for Information Systems. *A guide to business continuity management*. London: HMSO, 1995. ISBN 0-113-30675-X.

UNITED KINGDOM. Central Computer and Telecommunications Agency — the Government Centre for Information Systems. *An introduction to business continuity management*. London: HMSO, 1995. ISBN 0-113-30669-5.

UNITED KINGDOM. Civil Contingencies Secretariat, The Cabinet Office. *How resilient is your business to disaster?* London: HMSO, 1996.
See www.ukresilience.info/contingencies/business/resilient1.htm

UNITED KINGDOM. Civil Contingencies Secretariat, The Cabinet Office. *Dealing with disaster*. 3rd ed. London: HMSO, 2002.
See www.ukresilience.info/contingencies/dwd/

UNITED KINGDOM. Home Office. *Bombs: Protecting People and Property*. 4th ed. London: HMSO, 1999.
See www.homeoffice.gov.uk/oicd/bombs.pdf

UNITED KINGDOM. Office of Government Commerce. Chapter 9: IT service continuity management. In: *ITIL service delivery*. London: The Stationery Office, 2001.
ISBN 0-113-30017-4.

VON ROESSING, R. *Auditing business continuity: global best practices.* New York: Rothstein Associates Inc., 2002. ISBN 1-931-33215-0.

WESTMACOTT, P. Contingency planning: contractual issues. *Continuity*. 2001, **5** (1), 6–7.
See www.thebci.org

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 PAS would inform the Secretary of the technical committee responsible, the identity of which can be found in the foreword of this document. 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

BSI
389 Chiswick High Road
London
W4 4AL