

PAS 56

Guide to Business Continuity Management

ICS 03.100.01

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Insight
Consulting



This Publicly Available
Specification comes into
effect on 24 March 2003

© BSI 24 March 2003

ISBN 0 580 41370 5

Amd. No.	Date	Comments

Contents

	Page
Foreword	ii
Introduction	iii
1 Scope	1
2 Terms and definitions	1
3 Abbreviations	6
4 Overview	6
5 BCM programme management	7
6 Understanding your business	10
7 BCM strategies	14
8 Developing and implementing BCM plans	18
9 Building and embedding a BCM culture	21
10 BCM exercising, maintenance and audit	23
Annex A (informative) Participants in the BCM cycle	29
Annex B (informative) BCM evaluation criteria	31
Annex C (informative) Frequency and triggers	43
Bibliography	44
Figure 1 BCM — the unifying process	iii
Figure 2 BCM relationships	iii
Figure 3 The BCM lifecycle	7
Figure 4 The BIA and RA process	12
Figure 5 Exercising types and methods	24
Table A.1 RACI participants in the BCM cycle	30

Foreword

This Publicly Available Specification, PAS 56, was sponsored by the Business Continuity Institute¹ and Insight Consulting Limited², 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].

This Publicly Available Specification has been prepared and published by BSI, which retains its ownership and copyright. BSI reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

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

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.

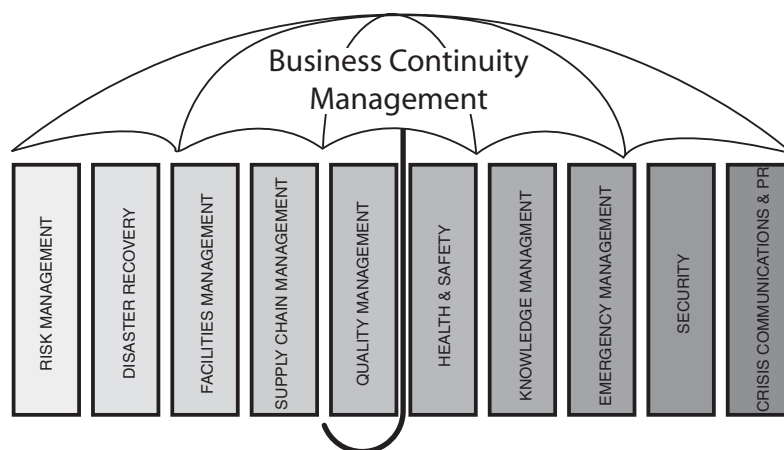


Figure 1 — BCM — the unifying process³

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.

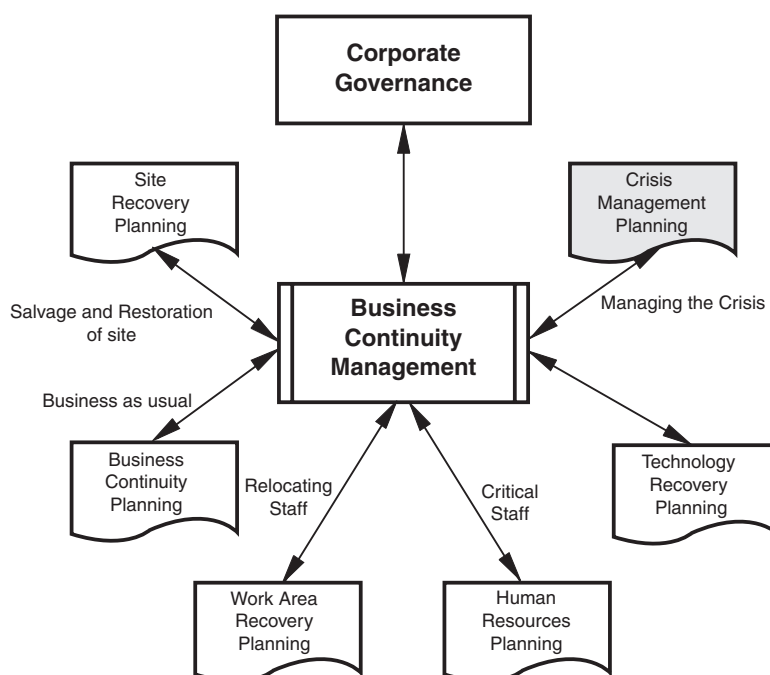


Figure 2 — BCM relationships⁴

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).

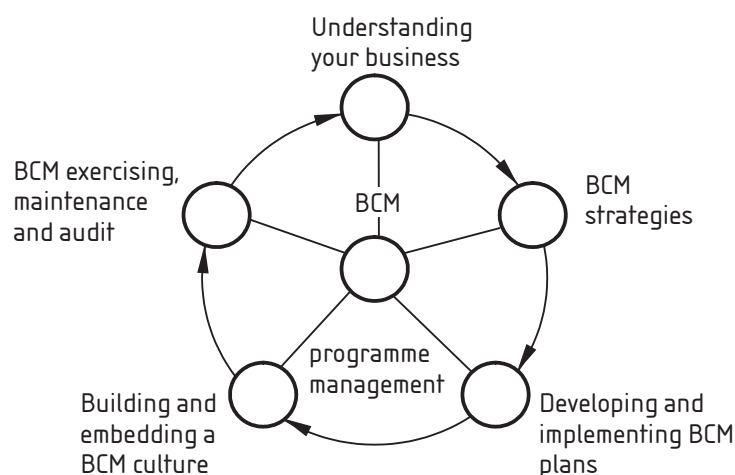


Figure 3 — The BCM lifecycle⁵

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.