

BRITISH STANDARD

Business continuity management – Part 1: Code of practice

ICS 03.100.01

Confirmed February 2012

BSi
British Standards

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Documents
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2006

ISBN 0 580 49601 5

The following BSI references relate to the work on this standard:

Committee reference BCM/1

Draft for comment 06/30139869 DC

Publication history

First published November 2006

Amendments issued since publication

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

Contents

Foreword *ii*

1	Scope and applicability	<i>1</i>
2	Terms and definitions	<i>1</i>
3	Overview of business continuity management (BCM)	<i>6</i>
4	The business continuity management policy	<i>10</i>
5	BCM programme management	<i>13</i>
6	Understanding the organization	<i>16</i>
7	Determining business continuity strategy	<i>21</i>
8	Developing and implementing a BCM response	<i>26</i>
9	Exercising, maintaining and reviewing BCM arrangements	<i>35</i>
10	Embedding BCM in the organization's culture	<i>40</i>

References *42*

List of figures

Figure 1 – The business continuity management lifecycle	<i>9</i>
Figure 2 – Incident timeline	<i>27</i>

List of tables

Table 1 – Types and methods of exercising BCM strategies	<i>37</i>
--	-----------

Summary of pages

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

Foreword

Publishing information

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

Association of British Certification Bodies
Association of British Insurers
Association of Chief Police Officers
Association of Insurance Risk Managers
Business Continuity Institute
Cabinet Office
Chief Fire Officers' Association (CFOA)
Continuity Forum
Coventry University
Department of Trade and Industry
Emergency Planning Society
Federation of Small Businesses
Financial Services Authority
Independent International Organization for Certification
Institute of Directors
Institute of Emergency Management
Institute of Internal Auditors
Institute of Risk Management
Intellect
Metropolitan Police
Securities Industry Business Continuity Management Group (SIBCMG)
Society of Industrial Emergency Services Officers (SIESO)
Survive

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

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

Use of this document

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

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

Presentation conventions

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

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

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

Contractual and legal considerations

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

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

1 Scope and applicability

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

This Standard provides a system based on BCM good practice.

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

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

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

2 Terms and definitions

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

2.1 activity

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

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

2.2 business continuity

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

2.3 business continuity management (BCM)

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

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

2.4 business continuity management lifecycle

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

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

2.5 business continuity management programme

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

2.6 business continuity plan (BCP)

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

2.7 business continuity strategy

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

2.8 business impact analysis

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

2.9 civil emergency

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

2.10 consequence

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

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

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

2.11 cost-benefit analysis

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

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

2.12 critical activities

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

2.13 disruption

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

2.14 emergency planning

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

2.15 exercise

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

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

2.16 gain

positive **consequence**

2.17 impact

evaluated consequence of a particular outcome

2.18 incident

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

2.19 incident management plan

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

2.20 invocation

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

2.21 likelihood

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

NOTE 1 Likelihood can be expressed qualitatively or quantitatively.

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

2.22 loss

negative **consequence**

2.23 maximum tolerable period of disruption

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

2.24 organization

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

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

NOTE 1 The arrangement is generally orderly.

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

2.25 products and services

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

2.26 recovery time objective

target time set for:

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

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

2.27 resilience

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

2.28 risk

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

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

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

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

2.29 risk appetite

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

2.30 risk assessment

overall process of risk identification, analysis and evaluation

2.31 risk management

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

2.32 stakeholders

those with a vested interest in an organization’s achievements

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

2.33 top management

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

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

3 Overview of business continuity management (BCM)

3.1 What is BCM?

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

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

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

3.2 BCM and organizational strategy

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

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

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

All these issues are of strategic concern to the organization.

3.3 BCM – the relationship with risk management

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

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

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

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

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

3.4 Why an organization should undertake BCM

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

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

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

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

3.5 The benefits of an effective BCM programme

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

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

3.6 The outcomes of an effective BCM programme

The outcomes of an effective BCM programme are that:

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

3.7 Elements of the business continuity management lifecycle

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

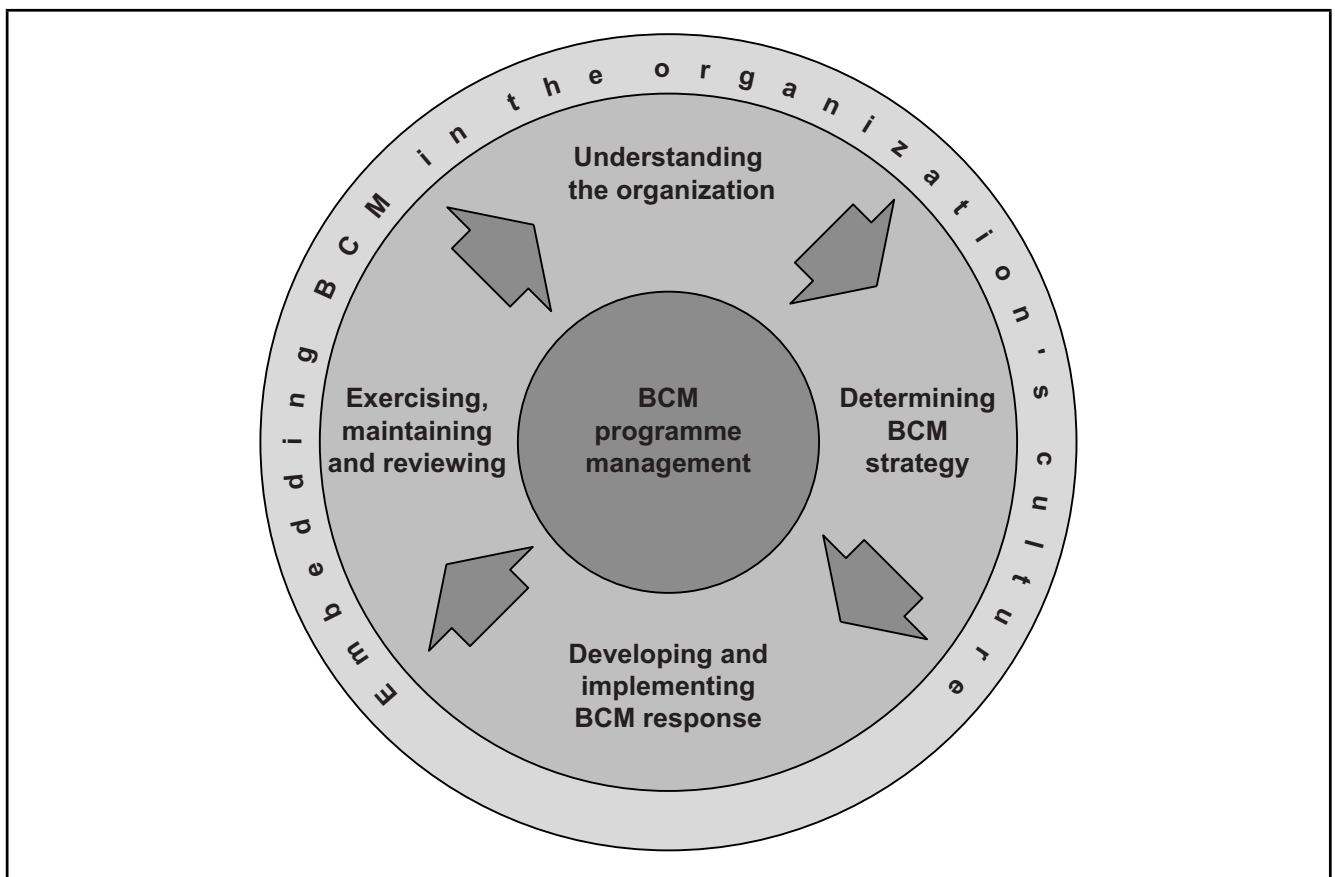
a) BCM programme management (see Clause 5)

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

b) Understanding the organization (see Clause 6)

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

Figure 1 The business continuity management lifecycle



c) Determining business continuity strategy (see Clause 7)

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

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

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