BS 25999-2:2007

BRITISH STANDARD

Business continuity management –

Part 2: Specification

ICS 03.100.01

British Standards

Publishing and copyright information

ISBN 978 0 580 59913 2

The following BSI references relate to the work on this standard:
Committee reference BCM/1
Draft for comment 07/30145272 DC

Publication history

First published November 2007

Amendments issued since publication

Amd. no.	Date	Text affected

Contents

Foreword *ii*
Introduction *1*

1 Scope *4*
2 Terms and definitions *4*
3 Planning the business continuity management system *9*
3.1 General *9*
3.2 Establishing and managing the BCMS *9*
3.3 Embedding BCM in the organization's culture *11*
3.4 BCMS documentation and records *11*
4 Implementing and operating the BCMS *12*
4.1 Understanding the organization *12*
4.2 Determining business continuity strategy *14*
4.3 Developing and implementing a BCM response *14*
4.4 Exercising, maintaining and reviewing BCM arrangements *16*
5 Monitoring and reviewing the BCMS *17*
5.1 Internal audit *17*
5.2 Management review of the BCMS *18*
6 Maintaining and improving the BCMS *19*
6.1 Preventive and corrective actions *19*
6.2 Continual improvement *20*

Annexes
Annex A (informative) Correspondence with BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005 *21*

Bibliography *23*

List of figures
Figure 1 – PDCA cycle applied to BCMS processes *2*
Figure 2 – The business continuity management lifecycle *3*

List of tables
Table A.1 – Correspondence of BS 25999-2 with other management systems standards *21*

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 23 and a back cover.

Foreword

This British Standard was published by BSI and came into effect on 20 November 2007. It was prepared by Panel BCM/1/-/2, under the authority of Technical Committee BCM/1, *Business continuity management*. A list of organizations represented on this committee can be obtained on request to its secretary.

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 define requirements for a management systems approach to business continuity management based on good practice for use in large, medium and small organizations operating in industrial, commercial, public and voluntary sectors.

BS 25999, *Business continuity management*, is published in two parts:

– *Part 1: Code of practice;*

– *Part 2: Specification.*

The requirements specified in this British Standard have been developed with due regard for the principles and practices contained within BS25999-1.

This British Standard provides a specification for use by internal and external parties, including certification bodies, to assess the organization's ability to meet regulatory, customer, and the organization's own requirements.

This British Standard contains only those requirements that can be objectively audited. Those organizations requiring more general guidance on a broad range of business continuity management issues are referred to BS 25999-1.

Demonstration of successful implementation of this British Standard can therefore be used by an organization to assure interested parties that an appropriate business continuity management system is in place.

In common with modern management system standards this standard utilizes the Plan-Do-Check-Act (PDCA) cycle for developing, implementing, and improving the effectiveness of an organization's business continuity management system.

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.

Introduction

General

This British Standard specifies requirements for setting up and managing an effective business continuity management system (BCMS).

This emphasizes the importance of:

a) understanding business continuity needs and the necessity for establishing policy and objectives for business continuity;

b) implementing and operating controls and measures for managing an organization's overall business continuity risks;

c) monitoring and reviewing the performance and effectiveness of the BCMS; and

d) continual improvement based on objective measurement.

A BCMS, like any other management system, has the following key components:

a) a policy;

b) people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review; and

   6) improvement;

d) a set of documentation providing auditable evidence; and

e) topic specific processes relating to the subject, in this case business continuity, such as business impact analysis (BIA) and business continuity plan development.

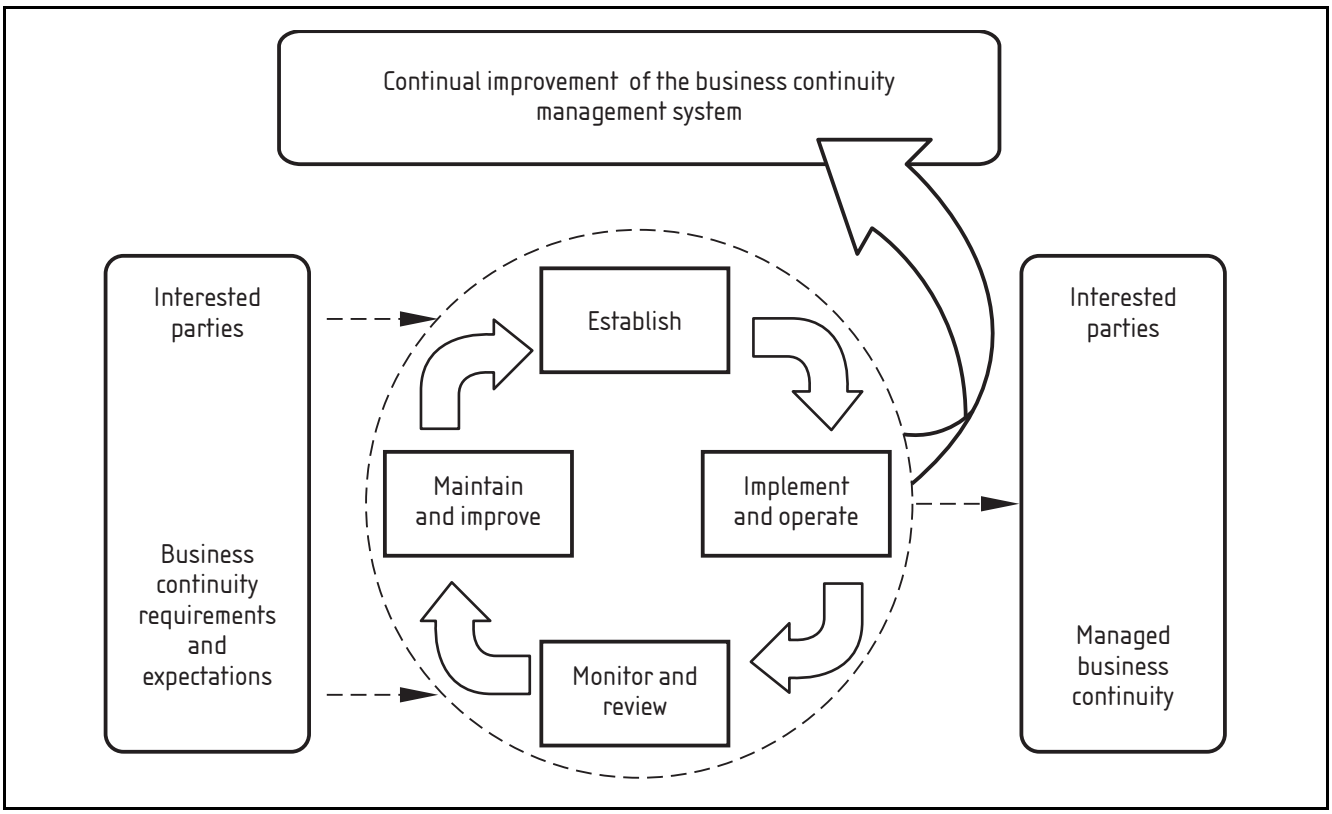
The Plan-Do-Check-Act (PDCA) cycle

The standard applies the "Plan-Do-Check-Act" (PDCA) cycle to establishing, implementing, operating, monitoring, exercising, maintaining and improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as BS EN ISO 9001:2000 (Quality Management Systems), BS EN ISO 14001:2004 (Environmental Management Systems), BS ISO/IEC 27001:2005 (Information Security Management Systems) and BS ISO/IEC 20000:2005 (IT Service Management), thereby supporting consistent and integrated implementation and operation with related management systems (see Annex A).

Figure 1 illustrates how a BCMS takes as inputs the business continuity requirements and expectations of the interested parties and, through the necessary actions and processes, produces business continuity outcomes (i.e. managed business continuity) that meet those requirements and expectations.

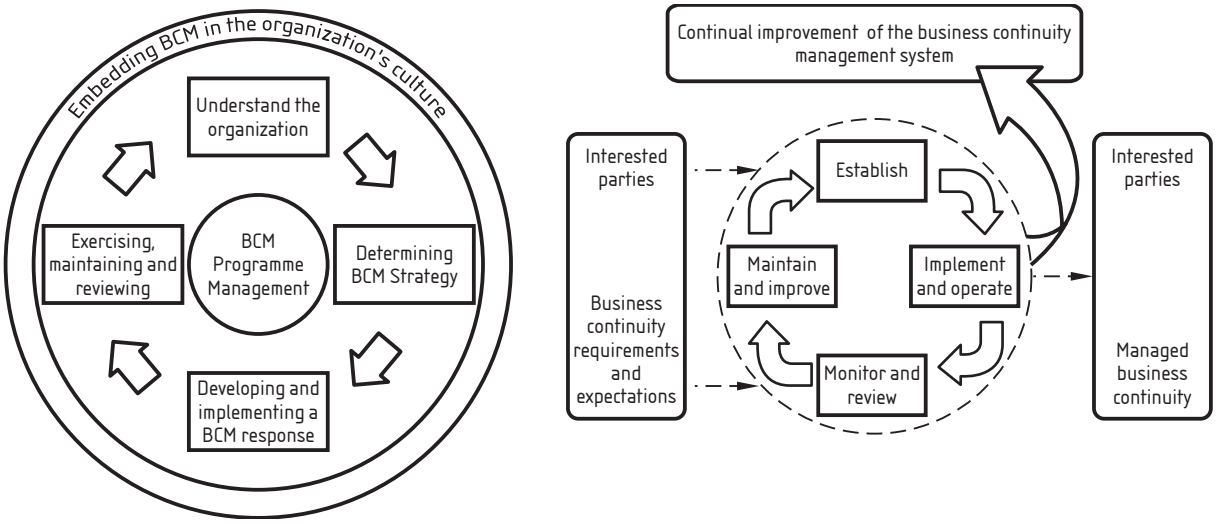
Figure 1 **PDCA cycle applied to BCMS processes**



Plan	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to managing risk and improving business continuity to deliver results in accordance with an organization's overall policies and objectives.
Do	Implement and operate the business continuity policy, controls, processes and procedures.
Check	Monitor and review performance against business continuity objectives and policy, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act	Maintain and improve the BCMS by taking preventive and corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

A widely accepted approach that incorporates the PDCA cycle within each activity is recommended in BS 25999-1 and summarized within Figure 2. This iterative process ensures that business continuity is established and continuously managed in an organization (for an explanation of each element of the business continuity management cycle, see BS 25999-1:2006, **3.7**).

Figure 2 **The business continuity management lifecycle**



The Business Continuity Lifecycle represents the continuous operation of the business continuity programme within the organization.	The PDCA cycle is the means of ensuring that business continuity is effectively managed and improved. The PDCA cycle applies to all parts of the BCM Lifecycle.

1 Scope

This British Standard specifies requirements for planning, establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving a documented BCMS within the context of managing an organization's overall business risks.

The requirements specified in this British Standard are generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of business. The extent of application of these requirements depends on the organization's operating environment and complexity.

It is not the intent of this British Standard to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets its stakeholders' requirements. These needs are shaped by regulatory, customer and business requirements, the products and services, the processes employed, the size and structure of the organization and the requirements of its stakeholders.

This British Standard can be used by internal and external parties, including certification bodies, to assess an organization's ability to meet its own business continuity needs, as well as any customer, legal or regulatory needs.

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 **organizatio**n (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 audit

systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's policy and objectives

[BS EN ISO 9000:2005]

2.3 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 predefined level

2.4 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.*

2.5 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 2.

2.6 business continuity management personnel
those assigned responsibilities defined in the BCMS, those accountable for BCM policy and its implementation, those who implement and maintain the BCMS, those who use or invoke the business continuity and **incident management** plans, and those with authority during an incident

2.7 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

2.8 business continuity management response
element of BCM concerned with the development and implementation of appropriate plans and arrangements to ensure continuity of **critical activities**, and the management of an incident

2.9 business continuity management system (BCMS)
that part of the overall **management system** that establishes, implements, operates, monitors, reviews, maintains and improves business continuity

*NOTE The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and **resources**.*

2.10 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 predefined level

2.11 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

2.12 business impact analysis (BIA)

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

2.13 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.

2.14 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.

2.15 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

2.16 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

2.17 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**.*

2.18 gain

positive **consequence**

2.19 impact

evaluated consequence of a particular outcome

2.20 incident

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

2.21 incident management plan (IMP)

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

2.22 internal audit
audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity

NOTE In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

2.23 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

2.24 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".

2.25 loss
negative **consequence**

2.26 management system
system to establish policy and objectives and to achieve those objectives

[BS EN ISO 9000:2005]

2.27 maximum tolerable period of disruption
duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed

2.28 nonconformity
non-fulfilment of a requirement

[BS EN ISO 9000:2005, **3.6.2**; BS EN ISO 14001:2004, **3.15**]

NOTE A nonconformity can be any deviation from relevant work standards, practices, procedures, legal requirements, etc.

2.29 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]

2.30 process
set of interrelated or interacting activities which transforms inputs into outputs

[BS EN ISO 9000:2005]

2.31 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

2.32 recovery time objective
target time set for resumption of product, service or activity delivery after an incident

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

2.33 resilience
ability of an organization to resist being affected by an incident

2.34 resources
all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives

2.35 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** 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.

2.36 risk assessment
overall process of **risk** identification, analysis and evaluation

2.37 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

2.38 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.

2.39 system
set of interrelated or interacting elements

[BS EN ISO 9000:2005]

2.40 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 Planning the business continuity management system

3.1 General

The **organization** shall develop, implement, maintain and continually improve a documented **BCMS** in accordance with **3.2** to **3.4**.

3.2 Establishing and managing the BCMS

Purpose

To define the boundaries of the BCMS, and to ensure that objectives are clearly stated, understood and communicated, **top management's** commitment to BCM is demonstrated, **resources** are allocated and those with BCM responsibilities are competent to perform their roles.

3.2.1 Scope and objectives of the BCMS

3.2.1.1 The organization shall define the scope of the BCMS and set **business continuity** objectives, with due regard to the:

a) requirements for business continuity;

b) organizational objectives and obligations;

c) acceptable level of **risk**;

d) statutory, regulatory and contractual duties; and

e) interests of its key **stakeholders**.

3.2.1.2 The organization shall identify the key **products and services** within the scope of the BCMS.

3.2.2 BCM policy

3.2.2.1 Top management shall establish and demonstrate commitment to a business continuity management policy.

3.2.2.2 The policy shall include or make reference to:

a) the organization's business continuity objectives; and

b) the scope of business continuity, including limitations and exclusions.

3.2.2.3 The policy shall be:

a) approved by top management; and

b) communicated to all persons working for or on behalf of the organization; and

c) reviewed at planned intervals and when significant changes occur.

3.2.3 Provision of resources

3.2.3.1 The organization shall determine and provide the resources needed to establish, implement, operate and maintain the BCMS.

3.2.3.2 BCM roles, responsibilities, competencies and authorities shall be defined and documented.

3.2.3.3 Top management shall:

a) appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation; and

b) appoint one or more persons, who, irrespective of other responsibilities, shall implement and maintain the BCMS.

3.2.4 Competency of BCM personnel

The organization shall ensure that all personnel who are assigned business continuity responsibilities are competent to perform the required tasks by:

a) determining the necessary competencies for such personnel;

b) conducting training needs analysis on personnel being assigned BCM roles and responsibilities;

c) providing training;

d) ensuring that the necessary competence has been achieved; and

e) maintaining records of education, training, skills, experience and qualifications.

3.3 Embedding BCM in the organization's culture

Purpose

To ensure that the organization embeds business continuity into its routine operations and management **processes**, regardless of its size or the sector within which it operates.

To ensure that BCM becomes a part of its core values and effective management, the organization shall:

a) raise, enhance and maintain awareness through an ongoing BCM education and information programme for all employees and establishing a process for evaluating the effectiveness of the BCM awareness delivery; and

b) communicate to all employees the importance of:

   1) meeting **business continuity management** objectives;

   2) conforming to the business continuity policy; and

   3) continual improvement; and

c) ensure that all employees are aware of how they contribute to the achievement of the organization's business continuity objectives.

3.4 BCMS documentation and records

Purpose

To provide clear evidence of the effective operation of the BCMS and the organization's implementation of BCM.

3.4.1 General

3.4.1.1 The organization shall have documentation covering the following aspects of the BCMS:

a) the scope and objectives of the BCMS and procedures (see **3.2.1**);

b) the BCM policy (see **3.2.2**);

c) the provision of resources (see **3.2.3**);

d) the competency of BCM personnel and associated training records (see **3.2.4**);

e) the **business impact analysis** (see **4.1.1**);

f) the **risk assessment** (see **4.1.2**);

g) the **business continuity strategy** (see **4.2**);

h) the incident response structure (see **4.3.2**);

i) **business continuity plans** and **incident management plans** (see **4.3.3**);

j) BCM exercising (see **4.4.2**);

k) the maintenance and review of BCM arrangements (see **4.4.3**);

l) **internal audit** (see **5.1**);

m) management review of the BCMS (see **5.2**);

n) preventive and corrective actions (see **6.1**); and

o) continual improvement (see **6.2**).

3.4.1.2 Records shall be established, maintained and controlled to provide evidence of the effective operation of the BCMS.

3.4.1.3 Documented procedures shall be established in order to identify the controls over BCMS documentation and records.

3.4.2 Control of BCMS records

Controls shall be established over BCMS records in order to:

a) ensure that they remain legible, readily identifiable and retrievable; and

b) provide for their identification, storage, protection and retrieval.

3.4.3 Control of BCMS documentation

Controls shall be established over BCMS documentation to ensure that:

a) documents are approved for adequacy prior to issue;

b) documents are reviewed and updated as necessary and re-approved;

c) changes and the current revision status of documents are identified;

d) relevant versions of applicable documents are available at points of use;

e) documents of external origin are identified and their distribution controlled; and

f) the unintended use of obsolete documents is prevented and that such documents are suitably identified if they are retained for any purpose.

4 Implementing and operating the BCMS

4.1 Understanding the organization

Purpose

To enable the organization to identify the **critical activities** and resources needed to support its key products and services, understand the threats to them and choose appropriate risk treatments.

4.1.1 Business impact analysis

4.1.1.1 There shall be a defined, documented and appropriate method for determining the **impact** of any **disruption** of the activities that support the organization's key products and services (see **3.2.1**).

4.1.1.2 The organization shall:

a) identify activities that support its key products and services;

b) identify impacts resulting from the disruption to these activities, and determine how these vary over time;

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

   1) the maximum time period after the start of a disruption within which each activity needs to be resumed;

   2) the minimum level at which each activity needs to be performed upon resumption; and

   3) the length of time within which normal levels of operation need to be resumed;

d) categorize its activities according to their priority for recovery and identify its critical activities;

e) identify all dependencies relevant to the critical activities, including suppliers and outsource partners;

f) for suppliers and outsource partners on whom critical activities depend, determine what BCM arrangements are in place for the relevant products and services they provide;

g) set **recovery time objectives** for the resumption of critical activities within their maximum tolerable period of disruption; and

h) estimate the resources that each critical activity will require for resumption.

4.1.2 Risk assessment

4.1.2.1 There shall be a defined, documented and appropriate method for risk assessment that will enable the organization to understand the threats to and vulnerabilities of its critical activities and supporting resources, including those provided by suppliers and outsource partners.

4.1.2.2 The organization shall understand the impact that would arise if an identified threat became an **incident** and caused a business disruption.

4.1.3 Determining choices

4.1.3.1 For each of its critical activities, the organization shall identify available risk treatments that:

a) reduce the **likelihood** of a disruption;

b) shorten the period of disruption; and

c) limit the impact of a disruption on the organization's key products and services.

4.1.3.2 The organization shall choose and implement appropriate risk treatments for each critical activity in accordance with its level of risk acceptance.

4.2 Determining business continuity strategy

Purpose

To identify BCM arrangements that will enable the organization to recover its critical activities within their recovery time objectives.

The organization shall:

a) define a fit-for-purpose, predefined and documented incident response structure that will enable an effective response and recovery from disruptions;

b) determine how it will recover each critical activity within its recovery time objective and the BCM arrangements, including the resources required for resumption and products and services provided by suppliers and outsource partners; and

c) determine how it will manage relationships with its key stakeholders and external parties involved in the recovery.

4.3 Developing and implementing a BCM response

Purpose

To enable the organization to develop and implement appropriate BCM plans and arrangements to manage any incident and continue its critical activities.

4.3.1 General

The organization shall use the outputs from **4.2** to develop and implement appropriate plans and arrangements to ensure continuity of critical activities and the management of an incident.

4.3.2 Incident response structure

4.3.2.1 The organization shall nominate incident response personnel with the necessary responsibility, authority and competence to manage an incident.

4.3.2.2 The incident response structure shall provide for personnel to:

a) confirm the nature and extent of an incident;

b) trigger an appropriate business continuity response;

c) have plans, processes and procedures for the activation, operation, coordination and communication of the incident response;

d) have resources available to support the plans, processes and procedures to manage an incident; and

e) communicate with stakeholders.

4.3.3 Business continuity plans and incident management plans

4.3.3.1 The organization shall have documented plans that detail how the organization will manage an incident and how it will recover or maintain its activities to a predetermined level in the event of a disruption.

4.3.3.2 Each plan shall:

a) have a defined purpose and scope;

b) be accessible to and understood by those who will use them;

c) be owned by a named person(s) who is responsible for their review, update and approval; and

d) be aligned with relevant contingency arrangements external to the organization.

4.3.3.3 The plans shall collectively contain:

a) identified lines of communications;

b) key tasks and reference information;

c) defined roles and responsibilities for people and teams having authority during and following an incident;

d) guidelines and criteria regarding which individuals have the authority to invoke each plan and under what circumstances;

e) a method by which each plan is invoked,

f) meeting locations with alternatives, and up-to-date contact and mobilization details for any relevant agencies, organizations and resources that might be required to support the response;

g) a process for standing down once the incident is over;

h) a reference to the essential contact details for all key stakeholders;

i) details to manage the immediate **consequences** of a business disruption giving due regard to:

   1) the welfare of individuals;

   2) strategic and operational options for responding to the disruption; and

   3) prevention of further **loss** or unavailability of critical activities;

j) details for managing an incident including:

   1) provision for managing issues during an incident; and

   2) processes to enable continuity and recovery of critical activities;

k) details on how and under what circumstances the organization will communicate with employees and their relatives, key stakeholders and emergency contacts;

l) details on the organization's media response following an incident, including:

   1) the incident communications strategy;

   2) preferred interface with the media;

   3) guideline or template for drafting a statement for the media; and

   4) appropriate spokespeople;

m) a method for recording key information about the incident, actions taken and decisions made;

n) details of actions and tasks that need to be performed;

o) details of the resources required for business continuity and business recovery at different points in time; and

p) prioritized objectives in terms of the critical activities to be recovered, the timescales in which they are to be recovered and the recovery levels needed for each critical activity.

4.4 Exercising, maintaining and reviewing BCM arrangements

Purpose

To verify the ongoing effectiveness of the BCM arrangements and to provide greater assurance following an incident that critical activities will be recovered as required.

4.4.1 General

The organization shall ensure that its BCM arrangements are validated by **exercise** and review and are kept up-to-date.

4.4.2 BCM exercising

4.4.2.1 The organization shall exercise its BCM arrangements to ensure that they meet business requirements.

4.4.2.2 The organization shall:

a) develop exercises that are consistent with the scope of the BCMS;

b) have a programme approved by top management to ensure exercises are carried out at planned intervals and when significant changes occur;

c) carry out a range of different exercises that taken together validate the whole of its business continuity arrangements;

d) plan exercises so that the risk of an incident occurring as a direct result of the exercise is minimized;

e) define the aims and objectives of every exercise;

f) carry out a post-exercise review of each exercise that will assess the achievement of the aims and objectives of the exercise; and

g) produce a written report of the exercise, outcome and feedback, including required actions.

4.4.3 Maintaining and reviewing BCM arrangements

4.4.3.1 The organization shall, at defined intervals, review its BCM arrangements to ensure their continuing suitability, adequacy and effectiveness.

4.4.3.2 The organization shall ensure its business continuity capability and appropriateness is reviewed at planned intervals and when significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

4.4.3.3 The review of BCM arrangements shall be regular and conducted either through self-assessment or audit.

4.4.3.4 In the event of an incident that results in the **invocation** of the BCP or the IMP, a post-incident review shall be undertaken to:

a) identify the nature and cause of the incident;

b) assess the adequacy of management's response;

c) assess the organization's effectiveness in meeting its recovery time objectives;

d) assess the adequacy of the BCM arrangements in preparing employees for the incident; and

e) identify improvements to be made to the BCM arrangements.

5 Monitoring and reviewing the BCMS

Purpose

To ensure that management monitor and review the effectiveness and efficiency of the BCMS, review the appropriateness of the business continuity policy, objectives and scope, and determine and authorize actions for remediation and improvement.

5.1 Internal audit

*NOTE The internal audit of the BCMS is distinct from the self-assessment or audit of the BCM arrangements specified in **4.4.3.3** (see also Note to **2.22**).*

5.1.1 The organization shall ensure that internal audits of the BCMS are conducted at planned intervals to:

a) determine whether the BCMS:

   1) conforms to planned arrangements for BCM, including the requirements of this BCM standard; and

   2) has been properly implemented and is maintained; and

   3) is effective in meeting the organization's BCM policy and objectives; and

b) provide information on the results of audits to management.

5.1.2 Any audit programme(s) shall be planned, established, implemented and maintained by the organization, taking into account the BIA, risk assessment, control and mitigation measures and the results of previous audits.

5.1.3 Audit procedure(s) shall be established, implemented and maintained that address:

a) the responsibilities, competencies and requirements for planning and conducting audits, reporting results and retaining associated records; and

b) the determination of audit criteria, scope, frequency and methods.

5.1.4 Selection of auditors and conduct of audits shall ensure objectivity and the impartiality of the audit process.

5.2 Management review of the BCMS

5.2.1 General

5.2.1.1 Management shall review the organization's BCMS at planned intervals and when significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

5.2.1.2 This review shall include assessing opportunities for improvement and the need for changes to the BCMS, including the business continuity management policy and business continuity management objectives.

5.2.1.3 The results of the reviews shall be clearly documented and records shall be maintained.

5.2.2 Review input

The input to a management review shall include information on:

a) results of BCMS audits and reviews, including where appropriate those of key suppliers and outsource partners;

b) feedback from interested parties, including independent observations;

c) techniques, products or procedures, which could be used in the organization to improve the BCMS performance and effectiveness;

d) status of preventive and corrective actions;

e) level of residual risk and acceptable risk;

f) vulnerabilities or threats not adequately addressed in the previous risk assessment;

g) follow-up actions from previous management reviews;

h) any internal or external changes that could affect the BCMS;

i) recommendations for improvement;

j) exercise results;

k) emerging good practice and guidance;

l) lessons from incidents; and

m) results of the education and awareness training programme.

5.2.3 Review output

The output from the management review shall include any decisions and actions related to:

a) varying the scope of the BCMS;

b) improving the effectiveness of the BCMS;

c) modification of BCM strategy and procedures, as necessary, to respond to internal or external events that could impact on the BCMS, including changes to:

1) business requirements;

2) **resilience** requirements;

3) business processes affecting the existing business requirements;

4) statutory, regulatory and contractual requirements; and

5) levels of risk and/or levels of risk acceptance;

d) resource needs; and

e) funding and budget requirements.

6 Maintaining and improving the BCMS

Purpose

To maintain and improve the effectiveness and efficiency of the BCMS by taking preventive and corrective actions, as determined by the management review.

6.1 Preventive and corrective actions

6.1.1 General

6.1.1.1 The organization shall improve the BCMS through the application of preventive and corrective actions.

6.1.1.2 Any preventive or corrective action taken shall be appropriate to the magnitude of the problems and commensurate with the business continuity policy and objectives.

6.1.1.3 Changes arising from preventive and corrective actions shall be reflected in the BCMS documentation.

6.1.2 Preventive action

The organization shall take action to guard against potential **nonconformities** in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

a) identifying potential nonconformities and their causes;

b) determining and implementing preventive action needed;

c) recording results of action taken;

d) reviewing preventive action taken;

e) identifying changed risks and ensuring that attention is focused on significantly changed risks;

f) ensuring that all those who need to know are informed of the nonconformity and preventive action put in place; and

g) the priority of preventive actions based on the results of the risk assessment and the BIA.

6.1.3 Corrective action

The organization shall take action to eliminate the cause of nonconformities associated with the implementation and operation of the BCMS in order to prevent their recurrence. The documented procedures for corrective action shall define the requirements for:

a) identifying any nonconformities;

b) determining the causes of nonconformities;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording the results of action taken; and

f) reviewing the corrective action taken.

6.2 Continual improvement

The organization shall continually improve the effectiveness of the BCMS through the review of the business continuity policy and objectives, audit results, analysis of monitored events, preventive and corrective actions, and management review.

Annex A (informative) Correspondence with BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005

Table A.1 shows the correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005 and BS 25999-2:2007.

Table A.1 **Correspondence of BS 25999-2 with other management systems standards**

BS 25999-2:2007	BS ISO/IEC 27001:2005	BS EN ISO 9001:2000	BS EN ISO 14001: 2004
Introduction	0 Introduction 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems	0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 compatibility with other management systems	Introduction
1 Scope	1 Scope 1.1 General 1.2 Application	1 Scope 1.1 General 1.2 Application	1 Scope
	2 Normative references	2 Normative reference	2 Normative references
2 Terms and definitions	3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
3 Planning the BCMS 3.1 General 3.2 Establishing and managing the BCMS	4 ISMS requirements 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS	4 QMS requirements 4.1 General requirements	4 EMS requirements 4.1 General requirements
4 Implementing and operating the BCMS 4.1 Understanding the organization 4.2 Determining business continuity strategy 4.3 Developing and implementing a BCM response	4.2.2 Implement and operate the ISMS		4.4 Implementation and operation
4.4 Exercising, maintaining and reviewing BCM arrangements	4.2.3 Maintain and improve the ISMS		4.5.1 Monitoring and measurement 4.5.2 Non-conformance and corrective and preventive action
3.4 BCMS documentation and records	4.3 Documentation requirements	4.2 Documentation requirements	
3.4.1 General	4.3.1 General	4.2.1 General 4.2.2 Quality manual	
3.4.2 Control of BCMS documentation 3.4.3 Control of BCMS records	4.3.2 Control of documents 4.3.3 Control of records	4.2.3 Control of Documents 4.2.4 Control of records	4.4.5 Documentation control 4.5.3 Records

Table A.1 **Correspondence of BS 25999-2 with other management systems standards** (*continued*)

BS 25999-2:2007	BS ISO/IEC 27001:2005	BS EN ISO 9001:2000	BS EN ISO 14001: 2004
	5 Management responsibility 5.1 Management commitment	5 Management responsibility 5.1 Management Commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	 4.2 Environmental policy 4.3 Planning
	5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competency	6 Resource management 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment	 4.2.2 Training, awareness and competence
5 Monitoring and reviewing the BCMS 5.2 Management review of the BCMS 5.2.1 General 5.2.2 Review input 5.3 Review output 5.1 Internal audit	6 Management review of the ISMS 6.1 General 6.2 Review input 6.3 Review output 6.4 Internal ISMS audits	5.6 Management review 5.6.1 General 5.6.2 Review input 5.6.3 Review Output 8.2.2 Internal audits	4.6 Management review 4.5.4 EMS audit
6 Maintaining and improving the BCMS 6.1 Preventive and corrective actions 6.2 Continual improvement 6.1.3 Corrective action 6.1.2 Preventive action	7 ISMS improvement 7.1 Continual improvement 7.2 Corrective action 7.3 Preventive action	8 Improvement 8.5.1 Continual improvement 8.5.2 Corrective actions 5.5.3 Preventive actions	 4.5.2 Non-conformance and corrective and preventive action
Annex A Correspondence with BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005	Annex A Control objectives and controls Annex B Guidance on use of the standard Annex C Correspondence between different management system standards	Annex A Links between ISO 14001:1996 and ISO 9001:2000	Annex A Guidance on use of the specification Annex B Links between ISO 14001:2004 and ISO 9001:2000

Bibliography

Standards publications

BS 25999-1:2006, *Business Continuity Management – Part 1: Code of Practice*

BS EN ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

BS EN ISO 9001:2000, *Quality management systems – Requirements*

BS EN ISO 14001:2004, *Environmental management systems – Specification with guidance for use*

BS ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*

BS ISO/IEC 20000-1:2005, *Information technology – Service management – Part 1: Specification*

BS ISO/IEC 20000-2:2005, *Information technology – Service management – Part 2: Code of practice*

BS ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO/IEC TR 13335-3:1998, *Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT security*

BS ISO/IEC TR 13335-4:2000, *Guidelines for the Management of IT Security – Part 4: Selection of safeguards*

ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*

ISO Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

Other publications

[1] OECD. *OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.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 British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

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

Buying standards

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

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

Information on standards

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

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

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

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

Copyright

389 Chiswick High Road
London
W4 4AL