

# BS 25999-2:2007 Business continuity management. Specification

(sample pages)

## Contents

|                                                                                                            |           |
|------------------------------------------------------------------------------------------------------------|-----------|
| Foreword                                                                                                   | <i>ii</i> |
| Introduction                                                                                               | 1         |
| <b>1</b> Scope                                                                                             | 4         |
| <b>2</b> Terms and definitions                                                                             | 4         |
| <b>3</b> Planning the business continuity management system                                                | 9         |
| <b>3.1</b> General                                                                                         | 9         |
| <b>3.2</b> Establishing and managing the BCMS                                                              | 9         |
| <b>3.3</b> Embedding BCM in the organization's culture                                                     | 11        |
| <b>3.4</b> BCMS documentation and records                                                                  | 11        |
| <b>4</b> Implementing and operating the BCMS                                                               | 12        |
| <b>4.1</b> Understanding the organization                                                                  | 12        |
| <b>4.2</b> Determining business continuity strategy                                                        | 14        |
| <b>4.3</b> Developing and implementing a BCM response                                                      | 14        |
| <b>4.4</b> Exercising, maintaining and reviewing BCM arrangements                                          | 16        |
| <b>5</b> Monitoring and reviewing the BCMS                                                                 | 17        |
| <b>5.1</b> Internal audit                                                                                  | 17        |
| <b>5.2</b> Management review of the BCMS                                                                   | 18        |
| <b>6</b> Maintaining and improving the BCMS                                                                | 19        |
| <b>6.1</b> Preventive and corrective actions                                                               | 19        |
| <b>6.2</b> Continual improvement                                                                           | 20        |
| <b>Annexes</b>                                                                                             |           |
| Annex A (informative) Correspondence with BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005 | 21        |
| Bibliography                                                                                               | 23        |
| <b>List of figures</b>                                                                                     |           |
| Figure 1 – PDCA cycle applied to BCMS processes                                                            | 2         |
| Figure 2 – The business continuity management lifecycle                                                    | 3         |
| <b>List of tables</b>                                                                                      |           |
| Table A.1 – Correspondence of BS 25999-2 with other management systems standards                           | 21        |

## Foreword

This British Standard was published by BSI and came into effect on 30 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.

|              |                                                                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Plan</b>  | 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. |
| <b>Do</b>    | Implement and operate the business continuity policy, controls, processes and procedures.                                                                                                                                                          |
| <b>Check</b> | 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.                                                |
| <b>Act</b>   | 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**).