ASIS INTERNATIONAL

Business Continuity Management Systems: Requirements with Guidance for Use

ASIS/BSI BCM.01-2010

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

BSI®

ASIS/BSI BCM.01-2010

an American National Standard

BUSINESS CONTINUITY MANAGEMENT SYSTEMS: REQUIREMENTS WITH GUIDANCE FOR USE

A management systems approach for preparedness and business/operational continuity management

Approved November 2, 2010

American National Standards Institute, Inc.

ASIS International and British Standards Institution (BSI)

Abstract

Based on the BS 25999 Business continuity management (Part 1 and Part 2), this *Standard* specifies requirements for a *business continuity management system (BCMS)* to enable an organization to identify, develop, and implement policies, objectives, capabilities, processes, and programs—taking into account legal and other requirements to which the organization subscribes—to address disruptive events that might impact the organization and its stakeholders. This *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 risks.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS International and BSI standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else. ASIS and BSI do not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

ASIS and BSI disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. ASIS and BSI disclaim and make no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. ASIS and BSI do not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS and BSI are not undertaking to render professional or other services for or on behalf of any person or entity, nor are ASIS and BSI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS and BSI have no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS and British Standards have no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS and British Standards do not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document shall not be attributable to ASIS and British Standards and is solely the responsibility of the certifier or maker of the statement. This publication does not purport to include all the necessary provisions of a contract. Compliance with a British Standard cannot confer immunity from legal obligations.

ISBN: 978-1-934904-07-7

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

ASIS International and BSI collaborated in the development of the *Business Continuity Management Systems: Requirements for Guidance for Use* Standard. This management systems standard provides generic auditable criteria and informative guidance on business continuity management.

About ASIS

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine – *Security Management* – ASIS leads the way for advanced and improved security performance.

The work of preparing standards and guidelines is carried out through the ASIS International Standards and Guidelines Committees, and governed by the ASIS Commission on Standards and Guidelines. The Mission of the ASIS Standards and Guidelines Commission is *to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry.*

About BSI

BSI is the UK's National Standards Body, recognized globally for its independence, integrity, and innovation in the production of standards and information products that promote and share best practices. BSI works with businesses, consumers, and government to represent UK interests and to make sure that British, European, and international standards are useful, relevant, and authoritative.

BSI Group is a global independent business services organization that inspires confidence and delivers assurance to customers with standards-based solutions. Originating as the world's first national standards body, the Group has over 2,300 staff operating in over 120 countries through more than 50 global offices.

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818, USA.

Commission Members

Jason L. Brown, Thales Australia
Steven K. Bucklin, Glenbrook Security Services, Inc.
John C. Cholewa III, CPP, Mentor Associates, LLC
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
Michael A. Crane, CPP, IPC International Corporation
William J. Daly, Control Risks Security Consulting
Eugene F. Ferraro, CPP, PCI, CFE, Business Controls Inc.
F. Mark Geraci, CPP, Purdue Pharma L.P., Chair
Robert W. Jones, Socrates Ltd, Inc.
Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair
John F. Mallon, CPP, Mallon & Associates, LLC
Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
John E. Turey, CPP, ITT Corporation
Roger D. Warwick, CPP, Pyramid International

At the time it approved this document, BCM Standards Committee, which is responsible for the development of this Standard, had the following members:

Committee Members

Committee Co-Chairman: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative, ASIS International
Committee Co-Chairman: Kevin S. Brear, J.P. Morgan Chase
Committee Secretariat: Sue Carioti, ASIS International
Committee Secretariat: David Adamson, British Standards Institution

David Adamson, British Standards Institution
Marene Allison, Johnson & Johnson
Edgard Ansola, Mutua Asepeyo
Paul H. Aube, CPP, Institut Grasset
Dave Austin, Operational Resilience Limited
Don Aviv, CPP, PCI, PSP, Interfor Inc.
William D. Badertscher, CPP, Georgetown University
Pradeep Bajaj, PRISMA
Thomas Bannister, Metropolitan Police Service
David Benish, Strategic BCP
Alan Berman, DRI International
Lyndon Bird, The Business Continuity Institute
Dennis R. Blass, CPP, PSP, Secumetrics LLC
John Boal, CPP, PCI, University of Akron
Mark Borchers, CPP, Germanna Community College
Thomas Bozek, Bozek Consulting, LLC
Kevin S. Brear, J.P. Morgan Chase
Patrick Brennan, BCMexperts
Larry Brown, First Citizens Bank
Frederick A. Budde, Ph.D., PCI, U.S. Department of Homeland Security, Federal Air Marshal Service
Doyle J. Burke, CPP, DAKO Group
Donald Byrne, North River Solutions
Thomas Carroll, Computer Sciences Corporation
Doug Cassell, Mutual of Enumclaw Insurance

Sharon Caudle Ph.D., The Bush School of Government and Public Service
Chee Seng Chan, Becton Dickinson Critical Care Systems Pte Ltd
Ian Charters, Continuity Systems Ltd
Telva Chase, Regence Group
Ian Clark, East Neuk Consultants Ltd
Justin Clarke, Gobanza, Inc.
Mike Claver, State Farm Insurance Companies
William Coffey, American Society of Safety Engineers
Andrew Collins, Baylor Health Care System
Malcolm Cornish, RMI (UK) Limited
Robert J. Coullahan, CEM, CPP, CBCP, Readiness Resource Group
Georges Cowan, Business Continu-IT Partners
Kevin Cunningham, UBS
Merlyn Demaine, Imperial College NHS Trust
Indrajit Dimyati, Business Continuity Planning Asia Pte Ltd
Brian Dixon, Moody International
Lisa DuBrock, The Radian Group, LLC
Robert Duncan, Consultant
Edward Eaton, Warner Gudlaugsson LLC
Henry Ee, Business Continuity Planning Asia Pte Ltd
Jorge Escalera, Risk Mexico
Greig Fennell, Sprint
Patti Fitzgerald, Disaster Recovery Journal
Windom Fitzgerald, Pendulum
Walter Fountain, CPP, Schneider National, Inc.
Christopher Frampton, SRCN Limited
Barry Freedman, FCS Consulting Services
Peter French, CPP, SSR Personnel
Robin Gaddum, IBM
Paul Genzburg, Soros Fund Management/Open Society Institute
Robert Giffin, Avalution Consulting
Stephen Giordano, HCA Inc.
Matthew Gneuhs, Cincinnati Children's Hospital Medical Center
Julia Graham, DLA Piper UK LLP
Briane Grey, U.S. Drug Enforcement Administration
Wayne Harrop, Centre for Disaster Management: Coventry University
Ronald Hauri, Northwestern University
John Hele, British Standards Institution
Michael Hill, Nokia
Andrea Hollman, United Space Alliance, LLC
Simon Honey, Mitsubishi UFJ Securities International plc.
Roger Housner, WPS Insurance Corporation
C.J. Howard, Deere & Company
Terri Howard, FEI Behavioral Health
David Huynh, Ross Stores, Inc.
Brian Kaye, Control Risks Group
David Kaye, Risk Reality
Michael Keating, Doulos Business Consulting
James Kennedy, Recovery-Solutions
Penelope Killow, HFC Bank (HSBC Group)
Steven King, CPP, U.S. Department of Homeland Security, Office of Infrastructure Protection
Paul Kirvan, Paul Kirvan Associates
Donald E. Knox, CPP, Caterpillar Inc.

Richard Kobylar, Capgemini
John Kunert, First Restoration
Michael Kuras, American Imaging Management, Inc.
Bill Lang, VCPI
Lince Lawrence, Allianz Cornhill Information Services
Grant Lecky, Citizenship and Immigration Canada
James J. Leflar Jr., CPP, CBCP, Johns Hopkins Bloomberg School of Public Health
Hugh Leighton, Aon Global Risk Consulting
Victoria Leighton, Avanade, Inc.
Eric Levine, Wellpoint
Wayne Lewis, Global Consulting
Judy Little, TSYS
William Lloyd, City National Bank
David Lloyd, The Business Continuity Institute
James Lukaszewski, The Lukaszewski Group Inc.
Bruce Lundeen, AT&T
Tracy Male, Bristol-Myers Squibb
Bill Marotz, Schneider National, Inc.
Andrew Mason, PricewaterhouseCoopers LLP
Diana McClure, Institute for Business & Home Safety
Richard McGlave, Continuity² Ltd
Jim McMahon, CPP, Align Technology
Mohamed Fadhel Meddeb, Efla Consultants Engineers
Cynthia Miller, Abbott
Murray Mills, CPP, New Zealand Ministry of Health
Susan Mitchell, Wilmer Cutler Pickering Hale and Dorr LLP
Goh Moh Heng, BCM Institute
Lawrence Mondschein, Consultant
Ashley Moore, Federal Emergency Management Agency, U.S. Department of Homeland Security
Dennis Morgan, CPP, International Consortium for Organizational Resilience
Richard Moulton, AlliedBarton
James Murphy, North Carolina Department of Health and Human Services
James Murray, Blue Cross and Blue Shield of Florida
Doug Nelson, Business Continuity Solutions
James Nelson, International Consortium for Organizational Resilience
Alan M. Nutes, CPP, Consultant
Kevin O'Donnell, UBS
Augustine O. Okereke, CPP, Statoil Nigeria Ltd
Philip Oppenheim, International Continuity Oversight Board
Mary Parrish, University of North Carolina at Chapel Hill
John A. Petruzzi Jr., CPP, Andrews International
Abigail Pollard, Blake Emergency Services
Jeanne Powell, IBM
Ren Powers, City National Bank
Werner Preining, CPP, Interpool Security Ltd
Russell Price, Continuity Forum
Daniel Puente Pérez, Sociedad de Prevención Asepeyo
Heidi Raffanello, KTM Strategies
Joseph Rector, CPP, PCI, PSP, United States Air Force
George Richards, CPP, Edinboro University of Pennsylvania
Robert Roberts, Federal Home Loan Bank of Atlanta
Jean Rowe, Verisign Inc.
Craig Rydalch, American Imaging Management, Inc.

Marilyn Saiewitz, Bristol-Myers Squibb
Angie Santiago, Contingency Planning Association of the Carolinas
Steve Schulze, WPS Insurance Corporation
Robert Sena, CPP, King's College
Chris Servia, University Health Systems of Eastern Carolina
John Sharp, Kiln House Associates Ltd
Daniel Shellenberger, Kinder Morgan
Robert Sherwood, North American Security Products Organization
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Lisa Smallwood, Comprehensive Emergency Management Professionals LLC
Thomas Smith, Comcast
Wolf Smith-Butz, Computer Sciences Corporation
Kurt Sohn, Capgemini
Ian Speirs, North Yorkshire County Council
Sam Stahl, EMC
Jim Stephens, The Royal Bank of Scotland
Stuart Sterling, HM Government (UK) Civil Contingencies Secretariat, Cabinet Office
Richard Taylor, Abu Dhabi Accountability Authority
Darryl Thibault, CPP, Pexis Corporation
Mike Thomson, Association of Contingency Planners
Raymond Trombley, Bank of Hawaii
Dave Tyson, CPP, Pacific Gas and Electric
Eric Van Balen, McKesson Corp.
Ray Van Hook, CPP, The School of The Art Institute
Suzanne Warner Hart, Delaware Department of Transportation
Lee Webster, Society for Human Resource Management
Douglas Weldon, Thomson Reuters
Renee Wentworth, Union First Market Bankshares
Carl Wertman, Mantech SRS Technologies
Robert Whitcher, BSI Management Systems America Inc.
Dan Wilder, Danalie Partners
Frederick Wilson, CBCP, Consulting
Amanda Witt, Booz Allen Hamilton
Zechariah Wei Ning Wong, Atkins
Mark Wright, Brookfield Properties
Tim Wright, Institute of Internal Auditors
Richard Wright, Wright Security, Inc.
Roberta Yang, The Yang Group
Lisa Zammit, Bank of England
Brian Zawada, Avalution Consulting

Working Group Members

Working Group Co-Chairman: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative, ASIS International

Working Group Co-Chairman: Kevin S. Brear, J.P. Morgan Chase

David Adamson, British Standards Institution
Pradeep Bajaj, PRISMA
Dennis R. Blass, CPP, PSP, Secumetrics LLC
Mark Borchers, CPP, Germanna Community College
Thomas Bozek, Bozek Consulting, LLC

Kevin S. Brear, J.P. Morgan Chase
Patrick Brennan, BCMexperts
Donald Byrne, North River Solutions
Chee Seng Chan, Becton Dickinson Critical Care Systems Pte Ltd
Ian Charters, Continuity Systems Ltd
Lisa DuBrock, The Radian Group, LLC
Edward Eaton, Warner Gudlaugsson LLC
John Hele, British Standards Institution
Brian Kaye, Control Risks Group
Michael Keating, Doulos Business Consulting
Penelope Killow, HFC Bank (HSBC Group)
Paul Kirvan, Paul Kirvan Associates
Donald E. Knox, CPP, Caterpillar Inc.
Richard Kobylar, Capgemini
Bill Lang, VCPI
Lince Lawrence, Allianz Cornhill Information Services
Mohamed Fadhel Meddeb, Efla Consultants Engineers
James Murphy, North Carolina Department of Health and Human Services
Doug Nelson, Business Continuity Solutions
James Nelson, International Consortium for Organizational Resilience
Alan M. Nutes, Consultant
Philip Oppenheim, International Continuity Oversight Board
Russell Price, Continuity Forum
Robert Roberts, Federal Home Loan Bank of Atlanta
Jean Rowe, Verisign Inc.
Angie Santiago, Contingency Planning Association of the Carolinas
Lisa Smallwood, Comprehensive Emergency Management Professionals LLC
Thomas Smith, Comcast
Kurt Sohn, Capgemini
Ian Speirs, North Yorkshire County Council
Stuart Sterling, HM Government (UK) Civil Contingencies Secretariat, Cabinet Office
Mike Thomson, Association of Contingency Planners
Suzanne Warner Hart, Delaware Department of Transportation
Renee Wentworth, Union First Market Bankshares
Dan Wilder, Danalie Partners
Zechariah Wei Ning Wong, Atkins
Brian Zawada, Avalution Consulting

TABLE OF CONTENTS

Table of Figures

TABLE OF TABLES

This page intentionally left blank

0 INTRODUCTION

0.1 General

A *business continuity management system (BCMS)* is an organization-wide process that establishes a fit-for-purpose, strategic, and operational framework that upon implementation by the organization's leadership:

- Improves an organization's ability to withstand disruptive events that may jeopardize the achievement of its purpose, mission, and strategic objectives.
- Delivers a demonstrable capability to manage a disruption and protect stakeholder interests.
- Provides a structured and rehearsed method of restoring an organization's productive ability within a planned timeframe after a disruption.
- Enables an organization to return to its normal state more quickly and safely than would otherwise be possible.
- Supports maintenance and continuous improvement of the organization's BCMS.
- Promotes the safety and security of internal and external stakeholders.

An actively engaged top management team that directs and embraces a BCMS enables an organization to create and maintain an effective and efficient business continuity program (processes, strategies, and solutions). The BCMS enables the organization to systematically address its stakeholder business continuity needs.

This *Standard* may be used by private, public, not-for-profit, and voluntary organizations, regardless of their size, scope, or complexity. The *Standard* accommodates diverse jurisdictional, geographical, cultural, operational, and social environments.

The success of a BCMS depends on the active engagement, endorsement, and commitment of organizational leadership to the BCMS. A BCMS enables an organization to develop a business continuity management policy, establish objectives and processes to achieve the policy commitments, and take action as needed for continual improvement of business continuity performance. A management system is a dynamic and iterative process; therefore, many of the requirements in this *Standard* may be addressed concurrently or revisited at any time.

A BCMS has the following base components:

a) A policy providing a framework for management's business continuity objectives and expectations;
b) A definition of roles, responsibilities, and resources;
c) A description of required management process relating to:
    i. Policy;
    ii. Strategic planning;
    iii. Business continuity planning and procedural implementation and operation;

iv. Performance assessment;
v. Management review; and
vi. Continual improvement.

d) A set of documentation providing auditable evidence demonstrating process implementation and repeatability.

The adoption and implementation of a range of business continuity management techniques in a systematic manner can contribute to optimal outcomes for all stakeholders and affected parties. However, adoption of this *Standard* will not by itself guarantee optimal preparedness, continuity, and response outcomes. In order to achieve its objectives, the BCMS should incorporate the best available practices, techniques, and technologies, where appropriate and where economically viable. The cost-effectiveness of such practices, techniques, and technologies should be taken fully into account.

This *Standard* does not establish absolute requirements for preparedness, response, continuity, or recovery performance beyond commitments in the organization's policy to:

a) Comply with applicable legal requirements and with other requirements to which the organization subscribes;
b) Support risk minimization and mitigation; and
c) Promote continual improvement.

The main body of this *Standard* contains only those generic criteria that may be objectively audited. Guidance on supporting BCM techniques is contained in the annexes of this document.

This *Standard*, like other management standards, is not intended to be used to create non-tariff trade barriers or to increase or change an organization's legal obligations. Indeed, conformance with a standard does not in itself confer immunity from legal obligations. Verification of an organization's conformance to this *Standard* may be performed through an external or internal auditing process. Verification may be by a first-, second-, or third-party mechanism. Verification does not require third-party certification.

This *Standard* does not include requirements specific to other management systems such as those for quality, occupational health and safety, or financial risk management—though its elements can be aligned or integrated with those of other management systems. It is possible for an organization to adapt its existing management system(s) in order to establish a BCMS that conforms to the criteria of this *Standard*. It should be understood, however, that the application of various elements of the management system might differ depending on the intended purpose and the stakeholder involved.

The level of detail and complexity of the BCMS, the extent of documentation, and the resources devoted to it will be dependent on a number of factors—such as the scope of the system; the

size of an organization; and the nature of its activities, products, and services. This may be the case in particular for small and medium-sized enterprises.

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

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. This *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.

Use of the PDCA model ensures a degree of consistency with other management systems standards, such as ISO 9001:2008 (Quality Management Systems), ISO 14001:2004 (Environmental Management Systems), ISO/IEC 27001:2005 (Information Security Management Systems), ISO 28000 (Security in the Supply Chain) and ISO/IEC 20000:2005 (IT Service Management), thereby supporting consistent and integrated implementation and operation with related management systems. A suitably designed management system can thus satisfy the requirements of all these standards (see Annex B). Organizations that have adopted an ISO approach to management systems may be able to use their existing management system as a foundation for the business continuity management system.

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.

NOTE: In practice, a PDCA cycle is applied to each stage of the BCMS process in an iterative approach.

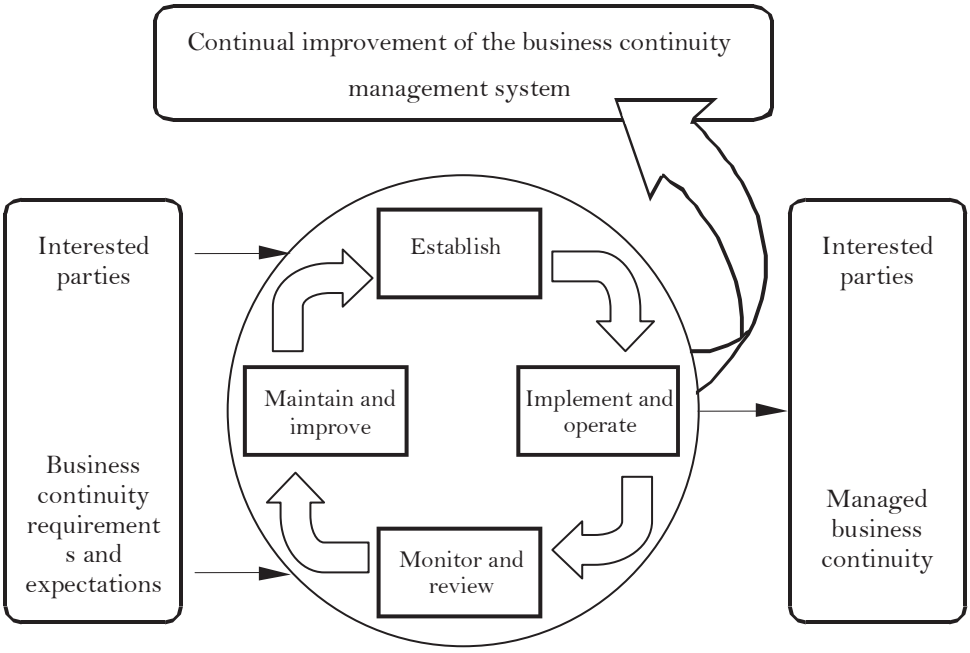

Figure 1: PDCA cycle applied to BCMS processes

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing business continuity risks and improving response and recovery processes that deliver results in accordance with the organization's strategic needs.
Do (implement and operate the management system)	Implement and operate the management system policy, controls, processes, and procedures.
Check (monitor and review the management system)	Monitor, assess, measure, and review performance against management system policy, objectives, and practical experience; report the results to management for review; and determine and authorize actions for remediation and improvement.
Act (maintain and improve the management system)	Take corrective and preventive actions, based on the results of the internal management system audit and management review, re-appraising the scope of the BCMS and business continuity policy and objectives to achieve continual improvement of the management system.

Conformance with this *Standard* can be verified by the auditing process described in ISO 19011:2002 that is compatible and consistent with the methodology used for ISO 9001:2008, ISO 14001:2004, ISO 28000:2007, and/or ISO/IEC 27001:2005, and the PDCA Model.

an American National Standard –

Business Continuity Management Systems: Requirements with Guidance for Use

1 SCOPE OF STANDARD

This *Standard* specifies requirements for a *business continuity management system (BCMS)* to enable an organization to identify, develop, and implement policies, objectives, capabilities, processes, and programs—taking into account legal and other requirements to which the organization subscribes or is governed by—to address disruptive events that might impact the organization and its stakeholders. This *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 risks.

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

This *Standard* seeks to offer a flexible management systems approach to address and minimize the consequences associated with disruptive events.

This *Standard* addresses all aspects of the organization deemed essential to meeting commitments (as agreed to by top management), consistent with the scope of the BCMS. The *Standard* does not itself state specific performance criteria.

The intent of this *Standard* is to position an organization to design a BCMS that is appropriate to its needs. These needs are shaped by customer and other stakeholder, regulatory, and operational requirements; the products and services; the processes employed; the size and structure of the organization; and jurisdictional and geographic areas of operation.

This *Standard* is applicable to any organization that chooses to:

a) Establish, implement, maintain, and improve a BCMS.
b) Assure itself of its conformity with its stated business continuity management policy.
c) Demonstrate conformity with this *Standard* by:
    i. Making a self-determination and self-declaration.
    ii. Seeking confirmation of its conformance by parties having an interest in the organization (such as customers and supply chain partners).
    iii. Seeking confirmation of its self-declaration by a party external to the organization.
    iv. Seeking certification/registration of its BCMS by an external organization.

Annex A provides informative guidance on management system planning, implementation, testing, maintenance, and improvement of a business continuity program.

2 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 General Reference[1]

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

3 TERMS AND DEFINITIONS

An extensive *Glossary* of terms appears in Annex D.

NOTE: The reader is encouraged to read through the terms and definitions prior to reading the body of the document.

4 BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) REQUIREMENTS

4.1 General Requirements

The organization shall establish, implement, operate, monitor, review, maintain, and improve a documented BCMS within the context of the organization's overall operational activities and the risks it faces. Figure 2 outlines the process specified by this Standard.

[1] This document is available from the International Organization for Standardization.
< http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >