ASIS INTERNATIONAL

Organizational Resilience: Security, Preparedness, and Continuity Management Systems–Requirements with Guidance for Use

ASIS SPC.1-2009

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS SPC.1-2009

an American National Standard for Security

ORGANIZATIONAL RESILIENCE: SECURITY, PREPAREDNESS, AND CONTINUITY MANAGEMENT SYSTEMS – REQUIREMENTS WITH GUIDANCE FOR USE

Approved March 12, 2009

American National Standards Institute, Inc.

Abstract

A comprehensive management systems approach for security, preparedness, response, mitigation, business/operational continuity, and recovery for disruptive incidents resulting in an emergency, crisis, or disaster.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

ASIS International 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 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 voluntary, nonprofit professional society with no regulatory, licensing or police power over its members. ASIS does not undertake a duty to third parties because it does not have the authority to enforce compliance with its standards. It assumes no duty of care to the general public, because its standards are not obligatory and because it does not monitor the use of those standards.

ASIS disclaims 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 disclaims and makes 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 does 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 is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS 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 has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has 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 does 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 is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-887056-92-2

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 (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests. 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, ASIS leads the way for advanced and improved security performance.

The work of preparing ASIS Standards is carried out through the ASIS International Standards and Guidelines Commission committees. Each member interested in a subject for which a technical committee has been established has the right to be represented on that committee.

The Guidelines Program of ASIS International has received a Designation award under the Support Anti-terrorism by Fostering Effective Technology Act of 2002 (the SAFETY Act) from the U.S. Department of Homeland Security. Specifically, the SAFETY Act designation limits ASIS' liability for acts arising out of the use of the guidelines in connection with an act of terrorism and precludes claims of third party damages against organizations using the guidelines as a means to prevent or limit the scope of terrorist acts.

The ASIS International *Organizational Resilience: Security, Preparedness and Continuity Management Systems Standard* incorporates the guidance provided in the ASIS International *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 2005*. For additional information, the *Business Continuity Guideline* should be consulted. This best practices standard provides generic auditable criteria and informative guidance on prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents with a potential to escalate into an emergency, crisis, or disaster.

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, Embarq Corporation

Cynthia P. Conlon, CPP, Conlon Consulting Corporation

Michael A. Crane, CPP, IPC International Corporation

Eugene F. Ferraro, CPP, PCI, CFE, Business Controls Inc.

F. Mark Geraci, CPP, Bristol-Myers Squibb Co., Chair

Robert W. Jones, Kraft Foods, Inc.

Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair

John F. Mallon, CPP

Marc H. Siegel, Ph.D, ASIS Security Management System Consultant

Roger D. Warwick, CPP, Pyramid International

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

Committee Members

Committee Chairman: Marc H. Siegel, Ph.D., ASIS Security Management System Consultant

Committee Secretariat: Sue Carioti, ASIS International

Paul H. Aube, CCP, Federation C.J.A.
Don Aviv, PSP, CPP, PCI, Interfor Inc.
William D. Badertscher, CPP, BMP, Georgetown University
Pradeep Bajaj, OSSIM
Jay C. Beighley, CPP, Nationwide Insurance
Dennis R. Blass, CPP, PSP, Sec Engineers University of Alabama
Thomas Bozek, Bozek Consulting LLC
Jerry Brashear, Ph.D., ASME
Jerry J. Brennan, Security Management Resources
Richard C. Bryant, CBCP, CSE, Verizon Communications
Frederick A. Budde, Federal Air Marshal Service
Doyle J. Burke, CPP, Delphi Corporation/Securitas
Sharon Caudle, Ph.D., Texas A&M University
Jorge L. Checo, Gap Inc.
Nancy A. Cohen, CPA, CITP, CIPP, AICPA
Leah A. Core, MBCP, Godaddy.com
Hugues Costes, ArcelorMittal FCE
Robert J. Coullahan, CPP, CEM, CBCP, Readiness Resource Group Inc.
Maria G. Dominguez, CPP, Bank of America
Warren C. Edwards, Oak Ridge National Laboratory
Eduard J. Emde, CPP, CISSP, Interseco
Linda J. Fite, CPP, University MN Medical Center Fairview
Steven Foster, CPP, PCI, Business Controls Inc.
David H. Gilmore, CPP, Colonial Safeguards Inc.
Jeffrey P. Grossmann, Esq., St Johns University
Steve Hather, Shadexi Consulting
Robert M. Hayworth, CPP, Titan America LLC
Ricky S. Henson, CPP, Headquarters, Federal Protective Service
John A. Hill, Ph.D, University of Denver
Michael Johnson, CISSP, CISM, HISP, Security Assurance Advisors, LLC
Linda J. Kelly, Vector Security, Inc.
Donald E. Knox, CPP, Caterpillar Inc.
Scott Kohsel, ROK Systems Inc.
Konstantinos Kyrifidis, CPP, PSP, Security Advisory
Robert F. Lang, CPP, Kennesaw State University
James J. Leflar Jr., CPP, CBCP, Johns Hopkins University
Edward M. Levy, CIT Group Inc.
Adam W. Loomis, Bechtel National Inc.
Kim M. Loy-Curto, PSP, G4S Technology
James E. Lukaszewski, The Lukaszewski Group Inc.
Raymond R. McGill, CPP, Care Security Systems
Benjamin P. McGregor, Visual Defence
James E. McNeil, CPP, Mayo Clinic
Mohamed F. Meddeb, Linuhonnun Consulting Eng.
David A. Moore, PE, CSP, AcuTech Consulting Group
Dante I. Moriconi, CPP, PSP, Administaff
Eric H. Morse, Morse, Lattice Semiconductor Corp.
Richard E. Moulton, CPP, PSP, AlliedBarton
Doug Nelson, EMS Solutions
Joseph C. Nelson, CPP, J Nelson, Consultant
Alan M. Nutes, CPP, Consultant
Augustine O. Okereke, CPP, St. Alphonsus Catholic Church
John A. Petruzzi, Jr., CPP, CISM, Simon Property Group
Daniel W. Phillips, PSP, Naval Undersea Warfare Center
Wade R. Pinnell, CPP, Huffmaster Crisis Response, LLC
Joseph L. Rector, CPP, PSP, PCI, USAF/316th Security Forces Squadron
Scott Richter, ANAB
Robert W. Rogalski, RAND Corporation
Bernard J. Scaglione, CPP, New York Presbyterian Hospital
Michael Severin, Securitas Security Services
Rose M. Shyman, Pricewaterhouse Coopers LLP
Austin L. Smith, Department of Homeland Security
Tony Webster Smith, Sustainability Pty Ltd.
David L. Stackleather, Circuit City Stores Inc.
Eugene C. Sticco, Jr., Shell International B V
Mark L. Theisen, CPP, Thrivent Financial
Penny Turnbull, Ph.D. CBCP, Marriott International Inc.
Stephen Twomey, Diamond Resorts International
Robert M. Weronik, CPP, CHPA, General Electric Company
Michele Yoder, Analex Corporation

Working Group Members

Working Group Chairman: Marc H. Siegel, Ph.D., ASIS Security Management System Consultant

William D. Badertscher, CPP, BMP, Georgetown University
Dennis R. Blass, CPP, PSP, Sec Engineers University of Alabama
Sharon Caudle, Ph.D., Texas A&M University
James J. Leflar Jr., CPP, CBCP, Johns Hopkins University
Doug Nelson, EMS Solutions
Alan M. Nutes, CPP, Consultant

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

0 INTRODUCTION

0.1 General

This management system *Standard* (referred to as the "*Standard*") has applicability in the private, not-for-profit, non-governmental, and public sector environments. It is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a disruptive incident (emergency, crisis, or disaster). It enhances an organization's capacity to manage and survive the event, and take all appropriate actions to help ensure the organization's continued viability. Regardless of the organization, its leadership has a duty to stakeholders to plan for its survival. The body of this document provides generic auditable criteria to establish, check, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.

This *Standard* is designed so that it can be integrated with quality, safety, environmental, information security, risk, and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards (see Annex B). Organizations that have adopted a process approach to management systems (e.g., according to ISO 9001:2000, ISO 14001:2004, and/or ISO/IEC 27001:2005) may be able to use their existing management system as a foundation for the organizational resilience (OR) management system as prescribed in this *Standard*.

0.2 Process Approach

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. A management system can provide the framework for continual improvement to increase the probability of enhancing security, preparedness, response, continuity, and resilience. It provides confidence to the organization and its customers that the organization is able to provide a safe and secure environment which fulfills organizational and stakeholder requirements.

This *Standard* adopts a *process approach* for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's organizational resilience (OR) management system. An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes and their management, can be referred to as a "process approach".

The process approach for OR management presented in this *Standard* encourages its users to emphasize the importance of:

a) Understanding an organization's risk, security, preparedness, response, continuity, and recovery requirements;

b) Establishing a policy and objectives to manage risks;

c) Implementing and operating controls to manage an organization's risks within the context of the organization's mission;

d) Monitoring and reviewing the performance and effectiveness of the OR management system; and

e) Continual improvement based on objective measurement.

This *Standard* adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the OR management system processes. The PDCA model is sometimes referred to as the APCI (Assess-Protect-Confirm-Improve) Model. Figure 1 illustrates how an OR management system takes as input the OR management requirements and expectations of the interested parties and through the necessary actions and processes produces risk management outcomes that meet those requirements and expectations. Figure 1 also illustrates the links in the processes presented in clause 4.

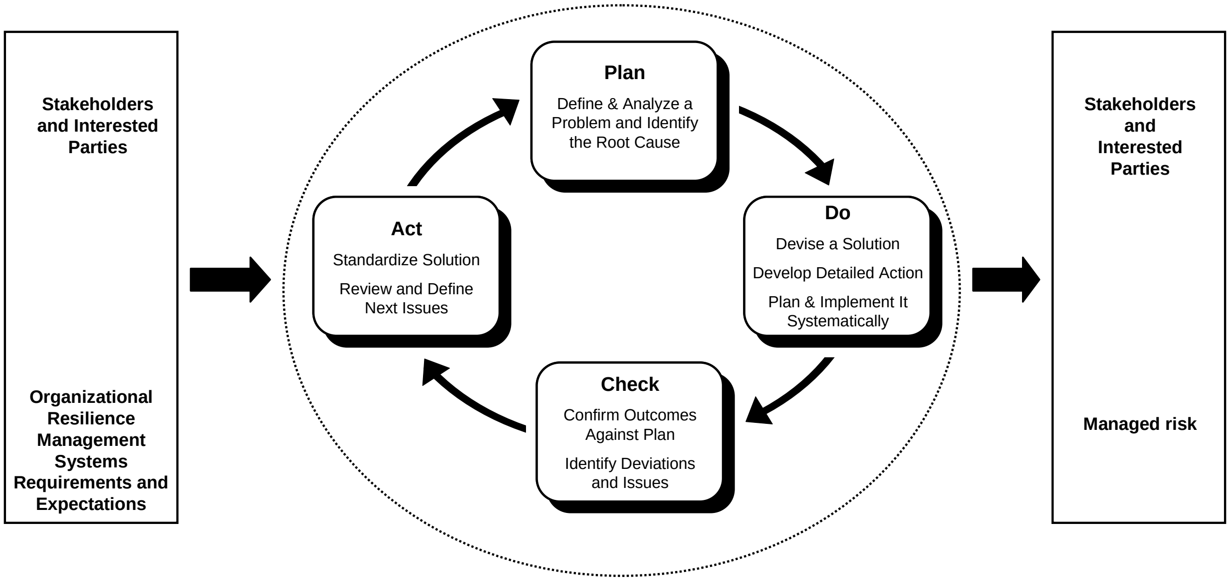
Stakeholders and Interested Parties
Organizational Resilience Management Systems Requirements and Expectations
Plan
Define & Analyze a Problem and Identify the Root Cause
Do
Devise a Solution
Develop Detailed Action
Plan & Implement It Systematically
Check
Confirm Outcomes Against Plan
Identify Deviations and Issues
Act
Standardize Solution
Review and Define Next Issues
Stakeholders and Interested Parties
Managed risk

Figure 1: Plan-Do-Check-Act Model

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing risk and improving security, incident preparedness, response, continuity, and recovery and to deliver results in accordance with an organization's overall policies and objectives.
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)	Assess and measure process performance against management system policy, objectives, and practical experience and report the results to management for review.
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, to achieve continual improvement of the management system.

Compliance with this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001:2000, ISO 14001:2004, and/or ISO/IEC 27001:2005, and the PDCA Model.

an American National Standard for Security –

Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use

1. SCOPE

This *Standard* specifies requirements for an organizational resilience (OR) management system to enable an organization to develop and implement policies, objectives, and programs taking into account legal requirements and other requirements to which the organization subscribes, information about significant hazards and threats that may have an impact on it (and its stakeholders'), and protection of *critical assets* (physical, intangible, environmental, and human). This *Standard* applies to risks and/or their impacts that the organization identifies as those it can control, influence, or reduce. It does not itself state specific performance criteria.

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

a) Establish, implement, maintain, and improve an OR management system;

b) Assure itself of its conformity with its stated OR management policy;

c) Demonstrate conformity with this *Standard* by:

   i. Making a self-determination and self-declaration; or

   ii. Seeking confirmation of its conformance by parties having an interest in the organization (such as customers); or

   iii. Seeking confirmation of its self-declaration by a party external to the organization; or

   iv. Seeking certification/registration of its OR management system by an external organization.

All the requirements in this *Standard* are intended to be incorporated into any type of organization's OR management system. It provides all the elements required to integrate management, technology, facilities, processes, and people into the resilience culture, risk management, and OR management system of an organization. The extent of the application will depend on factors such as the risk tolerance and policy of the organization; the nature of its activities, products, and services; and the location where, and the conditions in which, it functions.

This *Standard* provides generic requirements as a framework, applicable to all types of organizations (or parts thereof) regardless of size and nature of operation. It provides guidance for organizations to develop their own specific performance criteria, enabling the organization to tailor and implement an OR management system appropriate to its needs and those of its stakeholders.