

A S I S I N T E R N A T I O N A L

Maturity Model for the Phased Implementation of the Organizational Resilience Management System

ANSI/ASIS SPC.4-2012

AMERICAN NATIONAL STANDARD



an American National Standard

MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF THE ORGANIZATIONAL RESILIENCE MANAGEMENT SYSTEM

Approved February 2, 2012

American National Standards Institute, Inc.

ASIS International

Abstract

This Standard provides guidance for the use of a maturity model for the phased implementation of the ANSI/ASIS SPC.1-2009 organizational resilience standard in six phases, ranging from an unplanned approach, to managing events, to going beyond the requirements of the ANSI/ASIS SPC.1-2009 Standard and creating a holistic environment for resilience management.

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 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 does 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 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.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

Copyright © 2012 ASIS International

ISBN: 978-1-934904-30-5

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.

About ASIS

ASIS International (ASIS) is the preeminent organization for security professionals, with 38,000 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. An ANSI accredited Standards Development Organization, ASIS actively participates in the International Organization for Standardization. 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.*

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

Charles A. Baley, Farmers Insurance Group, Inc.
Jason L. Brown, Thales Australia
Steven K. Bucklin, Glenbrook Companies, 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
Lisa DuBrock, Radian Compliance
Eugene F. Ferraro, CPP, PCI, CFE, Business Controls, Inc.
F. Mark Geraci, CPP, Purdue Pharma L.P., Chair
Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc.
Robert W. Jones, Socrates Ltd
Glen Kitteringham, CPP, Kitteringham Security Group, Inc.
Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair
Bryan Leadbetter, CPP, Bausch & Lomb
Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

ANSI/ASIS SPC.4-2012

Jose M. Sobrón, United Nations
Roger D. Warwick, CPP, Pyramid International
Allison Wylde, London Metropolitan University Business School

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

Committee Members

Committee Chairman: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

Committee Secretariat: Sue Carioti, ASIS International

David Adamson, British Standards Institution
Paul H. Aube, CPP, Dessau
Pradeep Bajaj, PRISMA
Mark Baker, CPP, PCIP, MR Baker Security
Robert Ballagh, CPP, BCS Consulting LLC
Jay Beighley, Nationwide Insurance
Randy Bell, CPP, Securitas Security Services USA, Inc.
Lawrence Berenson, Consultant
Ray Bernard, PSP, RBCS Inc.
Dennis Blass, CPP, PSP, Children's of Alabama
Alan Borntrager, CPP, SAS
Bruce Braes, CPP, AECOM Australia Pty Ltd
Kevin Brear, JP Morgan Europe Ltd
Dan Breger, MSc AMBCI, Accenture
Christopher Burton, Avalution Consulting
Donald Byrne, Lead Auditor, CBCP, North River Solutions
Sharon Caudle, The Bush School, Texas A&M University
Chee Seng Chan, CBCP, Spot Management Services Pte Ltd
Hugues Costes, ArcelorMittal
Steve Crutchley, Consult2Comply
Jay Davidson, Royal Bank of Canada
Maria Dominguez, CPP, Bank of America
Lisa DuBrock, CPA, CBCP, Radian Compliance
Johan du Plooy, CPP, Temi Group
Michael Edgerton, Good Harbor Consulting
Jackie Finch, Iron Dragon, LLC
Sherryl Fraser, Algonquin College
John Gargett, TRUSYS
Millington Gumbo, ContinuitySA
Eddie L. Hall, Jr., CPP, Corporate Security Consultants & Mgt., LLC
Jon Hallaway, Harris County Hospital District
Caroline Hamilton, CHS III, RWInternational

.....

ANSI/ASIS SPC.4-2012

Suzanne Hart, Delaware Department of Transportation
Cal Jaeger, Ph.D., Sandia National Laboratories
Sue Kerr, Continuity First
Paul Kirvan, Paul Kirvan Associates
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Donald Knox, CPP, Caterpillar
Rich Kobylar, Capgemini
Henrik Laidlow-Petersen, Siemens Wind Power
Robert F. Lang, CPP, CEM, Kennesaw State University
Bill Lang, Independent Consultant
Grant Lecky, Department of Citizenship and Immigration Canada
James Leflar Jr., CPP, CBCP, Johns Hopkins Bloomberg School of Public Health
Petri Lillqvist, Finnair Plc
James Litchko, CISSP-ISSEP, CAP, MBCI, CMAS, Litchko & Associates, Inc.
Tracy Male, Bristol-Myers Squibb
Ronald Martin, CPP, Open Security Exchange
David McCoy, CPP, City of Austin
Sara McKenna, Continuity Forum
Gerald Mendes, CPP, GCL Services Limited
Dennis Morgan, CPP, Honeywell International
Jim Nelson, ICOR
Lynnda Nelson, Business Continuity Services, Inc.
Alan Nutes, CPP, Newell Rubbermaid
Philip Oppenheim, International Continuity Oversight Board
John Petruzzi, Jr., CPP, CISM, Andrews International
Russ Phillips, MMTS Group
Ann Pickren, Firestorm Solutions, LLC
Ren Powers, City National Bank
Russell Price, Ph.D., Continuity Forum
Loren Procter, Sprint Nextel
Bala Ramanan, Microland Ltd.
Scott Ream, Virtual Corporation
Joseph Rector, CPP, PSP, PCI, USAF/316th Security Forces Squadron
Thomas Rohr. Sr., CPP, Carestream
Craig Rydalch, American Imaging
Ed Schlichtenmyer, ImpactWeather
Johan Selle, iJET Intelligent Risk Systems
Ken Simpson, The VR Group P/L
Rajendra Singh, Wipro Limited
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Lisa Smallwood, CEMP, LLC
Thomas Smith, Comcast
Jose M. Sobrón, United Nations

Copyright ASIS International

ANSI/ASIS SPC.4-2012

Kurt Sohn, Capgemini
J. Kelly Stewart, Intelsat
Dan Straw, Pinkerton Government Services Inc.
Laurie Thomas, University of Findlay
Yoriko Tobishima, InterRisk Research Institute & Consulting, Inc.
Lina Tsakiris, CPP, TD Bank Group
Joop Verdonk, CPP, European Security Academy
Neil Wainman, CPP, E.ON UK
Kenji Watanabe, Ph.D., Nagoya Institute of Technology
Renee Wentworth, Independent Consultant
Allan Wick, CPP, PSP, CFE, Tri-State Generation & Transmission Association
Pauline Williams-Banta, PMP, MBCP, The Energy Authority
Gary Wilson, CPP, City of Vancouver
Wei Ning Zechariah Wong, Atkins
Tim Wright, Kingston Smith Consulting LLP
Allison Wylde, London Metropolitan University Business School
Jeffrey Zwirn, IDS Research & Development, Inc.

Working Group Members

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

Paul H. Aube, CPP, Dessau
Pradeep Bajaj, PRISMA
Dennis Blass, CPP, PSP, Children's of Alabama
Donald Byrne, Lead Auditor, CBCP, North River Solutions
Lisa DuBrock, CPA, CBCP, Radian Compliance
Johan du Plooy, CPP, Temi Group
Michael Edgerton, Good Harbor Consulting
John Gargett, TRUSYS
Millington Gumbo, ContinuitySA
Suzanne Hart, Delaware Department of Transportation
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Bill Lang, Independent Consultant
James Leflar Jr., CPP, CBCP, Johns Hopkins Bloomberg School of Public Health
James Litchko, CISSP-ISSEP, CAP, MBCI, CMAS, Litchko & Associates, Inc.
Jim Nelson, ICOR
Lynnda Nelson, Business Continuity Services, Inc.
Philip Oppenheim, International Continuity Oversight Board
Russ Phillips, MMTS Group
Ann Pickren, Firestorm Solutions, LLC
Ren Powers, City National Bank
Russell Price, Ph.D., Continuity Forum
Bala Ramanan, Microland Ltd.

ANSI/ASIS SPC.4-2012

Scott Ream, Virtual Corporation
Ed Schlichtenmyer, ImpactWeather
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Lisa Smallwood, CEMP, LLC
Jose M. Sobrón, United Nations
J. Kelly Stewart, Intelsat
Renee Wentworth, Independent Consultant
Pauline Williams-Banta, PMP, MBCP, The Energy Authority
Allison Wylde, London Metropolitan University Business School

Other Document Contributor(s)

Maya Siegel, Brandeis University

TABLE OF CONTENTS

0. INTRODUCTION.....	IX
0.1 GENERAL	IX
0.2 MANAGEMENT SYSTEMS APPROACH	X
1. SCOPE OF STANDARD.....	1
2. NORMATIVE REFERENCES	1
3. TERMS AND DEFINITIONS.....	2
4. MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF ANSI/ASIS SPC.1-2009	3
4.1 MATURITY MODEL.....	3
4.1.1 <i>What is a Maturity Model?</i>	3
4.1.2 <i>Why use a Maturity Model?</i>	4
4.1.3 <i>Using a Maturity Model with the Management Systems Approach</i>	4
4.2 PHASES OF THE MATURITY MODEL.....	5
4.2.1 <i>Phase One – Pre-awareness</i>	5
4.2.2 <i>Phase Two – Project Approach</i>	6
4.2.3 <i>Phase Three – Program Approach</i>	6
4.2.4 <i>Phase Four – Systems Approach</i>	7
4.2.5 <i>Phase Five – Management System</i>	7
4.2.6 <i>Phase Six – Holistic Management</i>	8
4.3. MATURITY MODEL MATRIX (MANAGEMENT SYSTEMS APPROACH)	8
A. USING THE MATURITY MODEL IN A RECOGNITION PROGRAM	25
B. BIBLIOGRAPHY.....	26

TABLE OF TABLES

TABLE 1: MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF THE ANSI/ASIS SPC.1-2009 ORGANIZATIONAL RESILIENCE STANDARD	9
--	---

0. INTRODUCTION

0.1 General

The Organizational Resilience Maturity Model is a methodology designed to implement organizational resilience concepts into core operating principles within any organization. This maturity model (referred to here as the “Standard”) for the phased implementation of the ANSI/ASIS SPC.1-2009 organizational resilience standard (referred to here as the “base 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.

Adopting a process for the phased implementation of an organization resilience management system (“maturity model”) helps the organization determine how much risk is acceptable and how to cost-effectively manage the uncertainty in achieving its objectives. Given the finite resources of organizations, it is imperative that they have tools to address the array of threats, hazards, and risks they may face. The maturity model described in this Standard helps organizations establish, implement, and maintain an Organizational Resilience Management System (ORMS) (e.g., ANSI/ASIS SPC.1-2009) to better manage the risks of potentially disruptive events through anticipation, prevention, protection, mitigation, response, and recovery.

This Standard identifies six phases of maturity to achieve continual improvement of organizational resilience through a management framework. The maturity model helps organizations achieve the benefits of resilience management by “phasing in” a system tied to the organization’s business needs and economic realities. The maturity model enhances an organization’s capacity to manage organizational resilience by avoiding, accepting, removing the source, changing the likelihood, changing the consequences, and sharing and/or retaining the risk. The body of this document provides auditable criteria to plan, do, check, and act, in order to drive continual improvement of the management system.

This model outlines six phases of implementation of the ANSI/ASIS SPC.1-2009 ranging from a pre-awareness phase (no process in place for resilience management) to holistic management (going beyond the requirements of the ANSI/ASIS SPC.1-2009), to promote resilience with stakeholders. Using this maturity model, an organization can achieve and maintain an appropriate level of resilience management as part of an organization’s culture.

The maturity model, for the phased implementation of the ANSI/ASIS SPC.1-2009, is a series of steps designed to help organizations evaluate where they currently are with regard to resilience management and preparedness, create a business or mission case, establish goals for achievement, benchmark where they are relative to those goals, and plot a reasonable business path to attain organizational resilience. Standards are designed to promote managed and repeatable performance. Managed and repeatable performance will be achieved by moving to a level appropriate for the organization, with the goal being to achieve the sixth step where possible.

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 maturity model for phased implementation can thus satisfy the requirements of other management systems standards. Organizations that have adopted a management system (e.g., according to ISO 9001:2000,

ISO 14001:2004, ISO 28000:2005, and/or ISO/IEC 27001:2005) can use this Standard in conjunction with their existing management systems.

0.2 Management Systems 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 prospect of enhancing anticipation, prevention, mitigation, response, and recovery. 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.

Through the full implementation, ongoing maintenance, and continual improvement of the ANSI/ASIS SPC.1-2009 organizational resilience management system, an organization is able to reach the ultimate goal of assuring organizational resilience. The phased approach recognizes that resilience must be aligned with the organization's needs and constraints in order to support continual improvement.

This American National Standard adopts a *process approach* for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's ORMS. An organization needs to identify and manage many activities in order to function effectively. Any activity using resources that is 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 maturity model approach for an ORMS presented in this Standard encourages its users to emphasize the importance of:

- a) Managing the organization's risk;
- b) Establishing a policy, objectives, and strategies to manage risks;
- c) Implementing controls to manage risks within the context of the organization's mission;
- d) Monitoring and reviewing the performance and effectiveness of the ORMS; and
- e) Continual improvement based on objective measurement.

The Maturity Model outlines six phases of implementation briefly described below as:

1. **Phase One:** *Pre-awareness* – Ad hoc resilience activities, no process currently in place, and resilience management is unstructured with no advanced preparation.
2. **Phase Two:** *Project Approach* – Commonly known as "the awareness phase", where management is willing to test the concept and establish a trial project to explore the benefits of resilience management and preparedness.
3. **Phase Three:** *Program Approach* – An expansion of the project approach. The organizational view begins to shift from specific issues to addressing division- or organization-wide issues implementing the core elements of the base standard.
4. **Phase Four:** *Systems Approach* – This phase involves integrating the core elements. Resilience management and preparedness are viewed as part of an iterative continual improvement process using the Plan-Do-Check-Act (PDCA) model.

ANSI/ASIS SPC.4-2012

5. **Phase Five: *Management System*** – All the core elements of the base standard have been applied and tested.
6. **Phase Six: *Holistic Management*** – Resilience management culture is well-developed and is considered an inseparable part of decision making.

The six phases of the model are focused on the phased implementation of a management system standard, all of which are applicable to any discipline or type of management system that seeks to treat risk. It is focused solely on organizational resilience utilizing balanced strategies to move from addressing just the minimization of consequences of a disruptive event to the procedures for anticipation, prevention, protection, preparedness, mitigation, and response and recovery appropriate to any organization or industry.

This page intentionally left blank.