

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

Security Management Standard: Physical Asset Protection

ANSI/ASIS PAP.1-2012

AMERICAN NATIONAL STANDARD



.....

an American National Standard

SECURITY MANAGEMENT STANDARD: PHYSICAL ASSET PROTECTION

Approved February 24, 2012

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard* presents a comprehensive management approach for the protection of assets by the application of security measures for physical asset protection.

This *Standard* may be used in conjunction with other ASIS International documents that provide additional information and details:

- ASIS International *Protection of Assets*.
- ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline*.
- ANSI/ASIS SPC.1-2009, *Organizational Resilience: Security Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*.

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: 978-1-934904-29-9

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 (SDO), 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 PAP.1-2012

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 PAP Standards Committee, which is responsible for the development of this *Standard*, had the following members:

Committee Members

Committee Co-Chair: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

Committee Co-Chair: Allison Wylde, London Metropolitan University Business School

Committee Secretariat: Sue Carioti, ASIS International

Walter Adams, CPP, AECOM
Sean Ahrens, CPP, BSCP, CSC, Aon
Christopher Aldous, CPP, PSP, Into Services Ltd
Azeem Aleem, University of Portsmouth
Michael Alexander, MSc, Henderson Global Investors
Edgard Ansola, CISA, CISSP, CEH, CCNA, ASEPEYO
Sue Armstrong, National Protection and Programs Directorate, DHS
Paul H Aube, CPP, Dessau
Pradeep Bajaj, Professional Industrial Security Management Academy
Debra Ballen, Institute for Business & Home Safety
Jay Beighley, CPP, CFE, Nationwide Insurance
Len Biegel, Fleishman-Hillard International Communications
Daniel Bierman, CPP, PSP, Whitman, Requardt & Associates
Dennis Blass, CPP, PSP, CFE, Children's of Alabama
Michael Bluestone, MA, Corps of Commissionaires Management Ltd t/a Corps Security
John Boal, CPP, PCI, CFE, University of Akron
Thomas Bolden, CPP, CAS, Capital One
Donald Byrne, CBCP, CDCP, Metrix411, LLC
Jim Castle, MSc, Corporate & Executive Solutions Ltd
Chee-Seng Chan, CBCP, Spot Management Services Pte Ltd
Ian Clark, F.B.C.I., East Neuk Consultants International Ltd.
Andrew Collins, CBCP, Baylor Health Care System
Michael Crocker, CPP, CSC, CPP & Associates, Inc.
Joe Davis, CPP, CFI, T-Mobile, USA
Jean-Marc Debon, CPP, Montreal International Airports

ANSI/ASIS PAP.1-2012

Russ Dempsey, Background Bureau, Inc.
Maria Dominguez, CPP, Bank of America
Jack Dowling, CPP, PSP, JD Security Consultants, LLC
Nicholas Economou, MBA, Cablevision Systems Corporation
James Ellis, MA, CPP, PSP, CSSM, CPO, Principal Financial Group
Jackie Finch, Iron Dragon, LLC
Phillip Guffey, CPP, Roche Diagnostics
Jon Hallaway, CHPA, Harris County Hospital District
Suzanne Hart, DHS ISSO, CBCP, Delaware Department of Transportation
Edward Heisler, CPP, PSP, Facility Control Systems, Inc.
Henri Hemery, RISK&CO
Alistair Hogg, CPP, Aotea Security Ltd
Mitchell Kemp, CPP, Cummins Filtration
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Stephen Krill Jr., CEM, PMP, CFCP, Booz Allen Hamilton
Henrik Laidlow-Petersen, Siemens Wind Power
Richard Lavelle, AIA, PSP, Reprise Design, Inc.
Bryan Leadbetter, CPP, CISSP, Bausch & Lomb
Alessandro Lega, CPP, Independent Consultant
Jeffrey Leonard, CPP, PSP, Securitas Security Services USA
Christopher Mark, MBA, American Sugar Refining Inc.
Ronald Martin, CPP, Open Security Exchange
Joseph McDonald, CPP, PSP, Switch Communications Group
Brian McDonough, CPP, Barclays Capital
William McGill, PE, CRE, The Pennsylvania State University
Jim McMahon, CPP, CISSP, Align Technology, Inc.
James McNeil, CPP, Mayo Clinic
Mohamed Fadhel Meddeb, Topic Energy
Robert Metscher, CPP, CFE, CISSP, Tacoma Goodwill Industries
Erin Mitchell, Agility Recovery Solutions
William Moore, PSP, Jacobs Global Buildings North America
Joseph Nelson, CPP, State Street
Henry Nocella, CPP, (DBA) Nocella Associates
Augustine O. Okereke, CPP, PZ Cussons PLC
Russ Phillips, MMTS Group
Roger Piper, CPP, Piper Consulting
Joseph Rector, CPP, PSP, PCI, USAF/11th Security Forces Group

ANSI/ASIS PAP.1-2012

Mark Riesinger, CPP, CHS-III, West Bend Mutual Insurance
James Saulnier, CPP, Sprint
Robert Schultheiss, CSC, Risk Decisions
Sarab Sembhi, CISSP, GCIH, ISACA, London
Robert Smart, CPP, EMQ Pty Ltd
Barry Stanford, CPP, AEG World Wide
Konstantinos Stergiopoulos, Nestle S.A.
Neil Stinchcombe, Eskenzi PR Ltd.
Paul Taibl, Business Executives for National Security
Mike Tennent, TAVCOM Ltd.
Theuns Van der Linde, SRK Consulting
Stéphane Veilleux, CPP, Pharmascience
Karim Vellani, CPP, CSC, Threat Analysis Group, LLC
Neil Wainman, CCP, E.ON UK
James Willison, MA, Unified Security Ltd.
Gavin Wilson, PSP, BHP Billiton
Loftin Woodiel, Ph.D., CPP, Woodiel Confidence Group
Allison Wylde, London Metropolitan University Business School

Working Group Members

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

Working Group Co-Chair: Allison Wylde, London Metropolitan University Business School

Walter Adams, CPP, AECOM
Christopher Aldous, CPP, PSP, Into Services Ltd
Dennis Blass, CPP, PSP, CFE, Children's of Alabama
John Boal, CPP, PCI, CFE, University of Akron
Michael Crocker, CPP, CSC, CPP & Associates, Inc.
Nicholas Economou, MBA, Cablevision Systems Corporation
James Ellis, MA, CPP, PSP, CSSM, CPO, Principal Financial Group
Phillip Guffey, CPP, Roche Diagnostics
Suzanne Hart, DHS ISSO, CBCP, Delaware Department of Transportation
Edward Heisler, CPP, PSP, Facility Control Systems, Inc.
Henri Hemery, RISK&CO
Mitchell Kemp, CPP, Cummins Filtration
Glen Kitteringham, CPP, Kitteringham Security Group Inc.

ANSI/ASIS PAP.1-2012

Richard Lavelle, AIA, PSP, Reprise Design, Inc.
Bryan Leadbetter, CPP, CISSP, Bausch & Lomb
Alessandro Lega, CPP, Independent Consultant
Jeffrey Leonard, CPP, PSP, Securitas Security Services USA
Ronald Martin, CPP, Open Security Exchange
Joseph McDonald, CPP, PSP, Switch Communications Group
James McNeil, CPP, Mayo Clinic
Mohamed Fadhel Meddeb, Topic Energy
William Moore, PSP, Jacobs Global Buildings North America
Henry Nocella, CPP, (DBA) Nocella Associates
Russ Phillips, MMTS Group
Roger Piper, CPP, Piper Consulting
James Saulnier, CPP, Sprint
Barry Stanford, CPP, AEG World Wide
Mike Tennent, TAVCOM Ltd.
James Willison, MA, Unified Security Ltd.
Gavin Wilson, PSP, BHP Billiton
Loftin Woodiel, Ph.D., CPP, Woodiel Confidence Group
Allison Wylde, London Metropolitan University Business School

UK Chapter

ASIS International acknowledges the contribution of the United Kingdom Chapter for preparing the starting point draft of this standard. This international effort was chaired by Allison Wylde, Technical Committee Co-chair, and included:

Executive Team

Christopher Aldous, CPP, PSP, Into Services Ltd
Gavin Wilson, CPP, BHP Billiton
Allison Wylde, FRGS, (DIC) Imperial, ASIS International Commission Standards and Guidelines

Starting Point Draft Team

Mike Alexander BEM, MSc, MSyL Henderson Global Investors
Graham Bassett MSyI, FIRP, FInstSMM, Managing Director, GBRUK Limited
Roger Bird, SGW Security Consulting
Chris Brogan, LLM, MSyL, Security SI
Helene Carlsson, Consultant
David Cresswell, MSc, CPP, PSP, ARC TC
Jim Castle MBE, MSc, FSyI, MIExpE, Corp & Executive Solutions Ltd
Tim Hodges, ASIS UK 208
Mike Hurst FIRP, MSyI, Director HJA Fire & Security Recruitment & Hurst Talent Acquisition

ANSI/ASIS PAP.1-2012

Letitia Emeana, PSP, Lloyds Banking Group
Mike White, FSyL
Neil Wainman, MSc, CPP, EON Ltd
Michael White, Consultant

Convergence Team

Alan Day, TFL
Alan Jenkins, CSC
Azeem Aleem, Portsmouth University,
Dave Tyson, CPP, MBA, Pacific Gas and Electric
David King Ph.D, Whimbrel Consulting
Alessandro Lega, CPP, ASIS Europe
James Willison MA, Unified Security Ltd.
Mike Bluestone, Principal Consultant, Corps Security, Chairman, The Security Institute
Neil Stinchcombe, Director Eskenzi PR Ltd
Paul Dorey Ph.D., CSO Confidential
Ken Heap, BP
Sarab Sembhi, CISSP, Incoming Thought
Martin Smith, MBE, The Security Company
Steve Thomas, BP
Simon Oxley, DPhil, Citicus
Steve Wright, PwC

TABLE OF CONTENTS

0. INTRODUCTION.....	XIII
0.1 ASSET PROTECTION	XIII
0.2 MANAGEMENT SYSTEMS APPROACH.....	XIV
1. SCOPE	1
2. NORMATIVE REFERENCES.....	1
3. TERMS AND DEFINITIONS	2
4. GENERAL PRINCIPLES	2
4.1 LEADERSHIP AND VISION.....	2
4.2 GOVERNANCE.....	2
4.3 NEEDS ORIENTED	3
4.4 SYSTEMS APPROACH.....	3
4.5 ADAPTABILITY AND FLEXIBILITY	3
4.6 MANAGING UNCERTAINTY	3
4.7 PHYSICAL ASSETS PROTECTION PERCEPTION	3
4.8 CONVERGENCE OF PERSPECTIVES.....	3
4.9 FACTUAL BASIS FOR DECISION MAKING	4
4.10 CONTINUAL IMPROVEMENT.....	4
5. LEADERSHIP AND GOVERNANCE.....	4
5.1 MANAGEMENT COMMITMENT	4
5.2 POLICY	4
6. ESTABLISHING THE FRAMEWORK	5
6.1 GENERAL	5
6.2 CONTEXT OF THE ORGANIZATION	5
6.2.1 External Context	5
6.2.2 Internal Context.....	6
6.2.3 Management Context	6
6.2.4 Scope of Physical Asset Protection Management System.....	6
A GUIDANCE ON THE INCORPORATION OF THIS STANDARD INTO THE ANSI/ASIS SPC.1-2009, ORGANIZATIONAL RESILIENCE MANAGEMENT SYSTEM STANDARD.....	8
A.1 GENERAL.....	8
A.2 SUPPORT	9
A.2.1 Resources	9
A.2.2 Communications and Consultations.....	9
A.3 DOCUMENTATION	10
A.3.1 Records.....	10
A.3.2 Control of Documents	10
A.4 PLANNING	11
A.4.1 Legal and Other Requirements	11
A.4.2 Risk Assessment and Application	12
A.4.2.1 Risk Identification and Exposure	13
A.4.2.2 Risk Treatment and Selection of Countermeasure Options.....	14
A.5 OBJECTIVES, TARGETS, AND PLANS TO ACHIEVE THEM	14
A.5.1 Physical Asset Protection Objectives and Targets.....	14
A.5.2 Physical Asset Protection Programs (Action Plans to Achieve Objectives).....	15
A.6 OPERATION AND IMPLEMENTATION.....	16

ANSI/ASIS PAP.1-2012

A.6.1	Resources, Roles, Responsibility, and Authority for Physical Asset Protection Management.....	16
A.6.2	Competence, Training, and Awareness.....	16
A.7	OPERATIONAL PROCEDURES AND CONTROLS.....	17
A.7.1	General.....	17
A.7.2	Documenting Procedures.....	18
A.7.3	Design of Controls and Countermeasures.....	19
A.7.4	Physical Protection Systems Lifecycle.....	20
A.7.5	Maintenance, Evaluation, and Replacement.....	21
A.7.6	Considerations for Emergency or Unusual Situations and Disruptive Events.....	22
A.8	PERFORMANCE EVALUATION.....	23
A.8.1	Monitoring and Measurement.....	23
A.8.2	Evaluation of Compliance.....	24
A.8.3	Exercises and Testing.....	24
A.8.4	Nonconformities; Corrective and Preventive Action.....	24
A.8.5	Internal Audit.....	25
A.9	MANAGEMENT REVIEW.....	25
A.10	IMPROVEMENT.....	26
A.10.1	Maintenance and Change Management.....	26
A.10.2	Continual Improvement.....	26
B	INFORMATIVE GUIDANCE ON THE ELEMENTS OF PHYSICAL ASSET PROTECTION.....	27
B.1	GENERAL.....	27
B.1.1	Process of Physical Asset Protection Systems Risk Assessment and Application.....	28
B.1.2	Security Survey.....	28
B.1.3	Cost Benefit Analysis.....	30
B.1.4	Security Convergence.....	31
B.1.5	Crime Prevention Through Environmental Design (CPTED).....	32
B.1.5.1	Implementation of CPTED.....	33
B.1.6	Site Hardening.....	34
B.1.6.1	Site Access and Perimeter Delineation.....	34
B.1.6.2	Implementation of Site Hardening Systems.....	34
B.2	SECURITY LIGHTING.....	35
B.2.1	Objectives of Security Lighting.....	35
B.2.2	Implementation of Security Lighting Systems.....	36
B.3	BARRIER SYSTEMS.....	36
B.3.1	Physical Barrier Systems.....	36
B.3.2	Implementation of Barrier Systems.....	37
B.4	INTRUSION DETECTION SYSTEMS.....	38
B.4.1	Objectives of Intrusion Detection Systems.....	39
B.4.2	Implementation of Intrusion Detection Systems.....	39
B.5	PHYSICAL ENTRY AND ACCESS CONTROL.....	40
B.5.1	Objectives of Entry and Access Control System.....	40
B.5.2	Implementation of Entry and Access Control Systems.....	41
B.6	VIDEO SYSTEMS - VIDEO SURVEILLANCE.....	42
B.6.1	Defining Parameters.....	42
B.6.2	Systems Architecture.....	43
B.6.3	Signal and Data Transmission.....	43
B.6.4	Recording Methods.....	44
B.6.5	System Ownership.....	44
B.6.6	Cameras.....	44
B.6.7	Direct Product Comparisons.....	45
B.6.8	Viewing Clients.....	45
B.6.9	System Design.....	46
B.6.10	Estimate.....	46

ANSI/ASIS PAP.1-2012

B.6.11	Procure and Install	47
B.6.12	Training	47
B.6.13	Policies and Procedures for System Use	48
B.6.14	Testing.....	48
B.7	ALARMS, COMMUNICATIONS, AND DISPLAY	48
B.7.1	Objectives of Alarms, Communications, and Display	49
B.7.2	Implementation of Alarms Monitoring, Communications, and Display Systems	49
B.7.2.1	Security.....	49
B.7.2.2	Technology	49
B.7.2.3	Architectural.....	50
B.7.2.4	Technical Systems	50
B.8	PERSONNEL.....	50
B.9	SECURITY POLICIES AND PROCEDURES	52
C	TERMS AND DEFINITIONS.....	53
D	BIBLIOGRAPHY	61

TABLE OF FIGURES

FIGURE 1: PLAN-DO-CHECK-ACT MODEL.....	XV
FIGURE 2: ORGANIZATIONAL RESILIENCE (OR) MANAGEMENT SYSTEM FLOW DIAGRAM.....	9
FIGURE 3: RISK ASSESSMENT AND TREATMENT PROCESS FLOW DIAGRAM BASED ON ISO 31000:2009.....	13

This page intentionally left blank.

0. INTRODUCTION

Protecting the assets of any organization – public, private or not-for-profit – is a critical task for the viability, profitability, reputation, and sustainability of the organization. This transcends the protection of just human and physical assets, and includes the securing of vital intellectual property and information. Protecting assets requires a combination of strategic thinking, process management, and the ability to implement programs and initiatives in increasingly shorter periods of time to match the rapid pace of today's global business environment.

This *Standard* provides an approach to identify, apply, and manage physical security measures to safeguard an organization's assets – people, property, information, and intangibles that are based in facilities (not during transit). Physical asset protection (PAP) – also known as physical security management – includes the protection of both tangible (e.g., physical, human, infrastructure, and environmental assets) and intangible assets (e.g., brand, reputation, and information assets). This *Standard* provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving physical protection systems (PPS).

All organizations face a certain amount of risk. The challenge is to determine how much risk is acceptable, and how to cost-effectively manage the risk while meeting the organization's strategic and operational objectives. Thus, choices must be made regarding the trade-off between the resources necessary to generate products, profits, and market-share, and the controls required to protect them. Successful asset protection provides the appropriate balance between these competing demands. This *Standard*, used in conjunction with the ASIS International *Protection of Assets* and the ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline*, will assist organizations in achieving this difficult balance in determining the appropriate level of acceptable risk for a broad variety of situations and the investment required to manage those risks.

This *Standard* views asset protection from the larger gamut of risk and resilience management as it relates to the complete protection of assets. The management system used in this *Standard* is the framework presented in the ANSI/ASIS SPC.1-2009, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use* Standard. This *Standard* provides informative guidance on incorporating the elements of asset protection into the Organizational Resilience Management System (ORMS).

This *Standard* is designed so that it can be integrated with quality, safety, environmental, information security, supply chain security, organizational resilience, risk, and other management systems standards within an organization. A suitably designed management system can thus satisfy the requirements of all these standards.

0.1 Asset Protection

The context of asset protection – when applied to a *physical asset protection management system (PAPMS)* – considers risks associated with intentional, unintentional, and/or naturally caused events. Asset protection incorporates the organization's security and related functions (e.g., risk management, safety, finance, quality assurance, compliance, etc.) into a comprehensive, proactive management system.

Asset protection is directly tied to the organization's mission to protect its tangible and intangible assets by removing or reducing exposure to the causes and consequences of risks.

The organization's management system should:

- a) Ensure top management leadership and commitment to the PAP policy;
- b) Establish a comprehensive risk management program that identifies, analyzes, and evaluates risks to tangible and intangible assets;
- c) Characterize the assets, design, and implement a PPS that meets the objectives against the available resources;
- d) Integrate people, procedures, technologies, and equipment to meet the objectives; and
- e) Continuously monitor, measure, and review the performance of the management system.

In order to effectively protect its assets, an organization needs to recognize the interdependencies of various business functions and processes to develop a holistic approach to PAP. Physical asset protection is intertwined with other security-related disciplines, such as information technology systems and continuity management. In order to understand the shared risk environment, the organization should consider:

- a) A common basis for risk ownership and accountability;
- b) An integrated risk assessment and harmonized treatment strategy;
- c) Common lines of communications and reporting for assessing and managing risk in a cross-disciplinary and cross-functional fashion; and
- d) Establishing cross-disciplinary and cross-functional teams to achieve a coordinated pre-emptive and response structure.

When implementing this *Standard*, organizations should adopt a comprehensive and integrated strategy that encompasses all areas of security risk. This should be reflected in all elements of the *Standard*. The organization will be better able to achieve its objectives by understanding and integrating PAP, information technology systems, and risk management in all of the elements of its management system.

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 probability of enhancing security and asset protection. It provides confidence to the organization, and its customers, that it can provide a safe and secure environment which fulfills organizational and stakeholder requirements.

This *Standard* adopts a management systems approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's PAPMS. 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 management systems approach is a set of interrelated elements and processes within an organization. By understanding the interrelationships between the elements and processes, the organization is able to implement its policy and achieve its objectives of managing asset protection. The management systems approach for PAP management presented in this *Standard* encourages its users to emphasize the importance of:

- Understanding the organization's context, risk, and PAP requirements;
- Establishing a policy and objectives to manage risks;
- Implementing, operating, and maintaining controls to manage an organization's risks within the context of the organization's mission;
- Monitoring and reviewing the performance and effectiveness of the PAPMS; and
- Ensuring continual improvement based on objective measurement.

This *Standard* adopts the "Plan-Do-Check-Act" (PDCA) model, used in the ANSI/ASIS SPC.1-2009, which is applied to structure the PAPMS processes. Figure 1 illustrates how ANSI/ASIS SPC.1-2009 and PAPMS takes as input the PAP 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 this *Standard*.

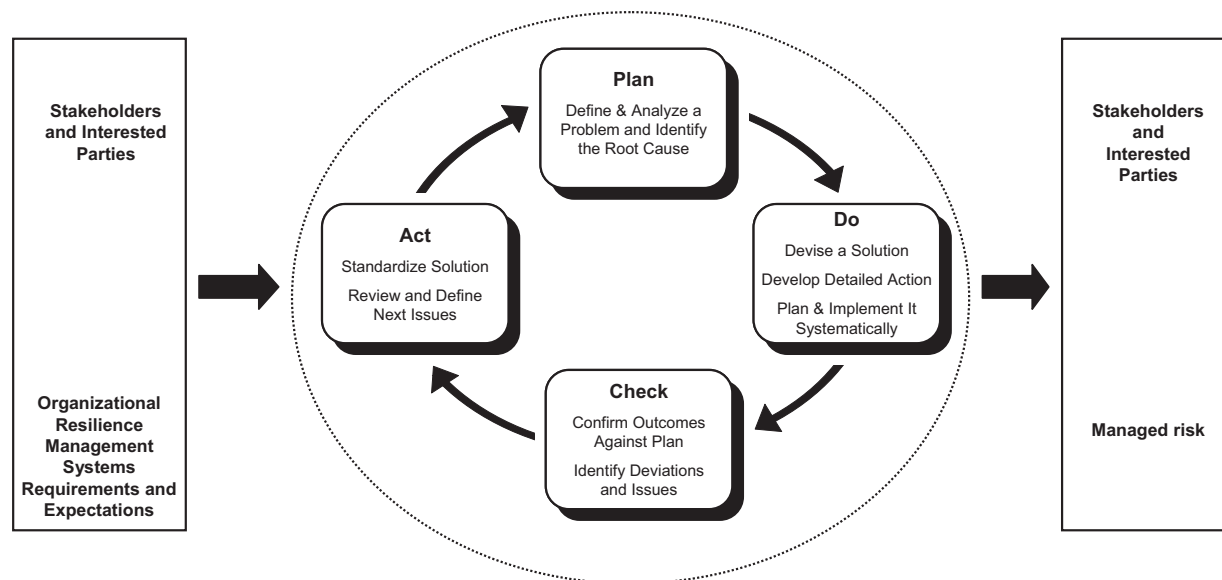


Figure 1: Plan-Do-Check-Act Model

ANSI/ASIS PAP.1-2012

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing risk and improving security risk management and PAP, 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.

Conformance to this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of other management systems standards – ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005, ISO 28000:2007, ANSI/ASIS SPC.1-2009, and the PDCA Model. This *Standard* uses the risk management approach of ISO 31000: 2009.

Security Management Standard: Physical Asset Protection

1. SCOPE

This *Standard* provides generic principles, requirements, and guidance as well as the framework for a management system to assist organizations in the design, implementation, monitoring, evaluation, maintenance, and replacement of PPS. All the requirements and guidance in this *Standard* are intended to be incorporated in ANSI/ASIS SPC.1-2009, or any type of an organization's management system based on the PDCA model. The *Standard* is applicable to organizations of all sizes across all sectors: private, public and not-for-profit.

A PAPMS includes the protection of both tangible and intangible assets.

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

- a) Establish, implement, maintain, and improve the PAPMS;
- b) Confirm conformity with its stated PAP and management policy;
- c) Commit to continual improvement through duty of care; and
- d) 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); or
 - III. Seeking confirmation of its self-declaration by an external party.

This *Standard* provides generic principles, requirements, and guidance intended to be incorporated into any organization-wide risk and resilience management system (see ANSI/ASIS SPC.1-2009) intended to minimize the risks of disruptive events; it is not intended to promote a uniform approach to all organizations in all sectors. The design, implementation, and evaluation of PAP plans, procedures, and practices should take into account the particular requirements of each organization: its objectives, context, customers, culture, structure, assets, operations, processes, products, and services – as well as financial and regulatory realities.

2. NORMATIVE REFERENCES

The following documents contain information which, through reference in this text, constitutes foundational knowledge for the use of this American National Standard. At the time of publication, the editions indicated were valid. All material is subject to revision, and parties are encouraged to investigate the possibility of applying the most recent editions of the material indicated below.

ANSI/ASIS SPC.1-2009, *Organizational Resilience: Security Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*.

ISO Guide 73:2009, *Risk Management – Vocabulary*.

ISO 31000:2009, *Risk Management – Principles and Guidelines*.

3. TERMS AND DEFINITIONS

An extensive Glossary of terms appears in Annex C.

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

4. GENERAL PRINCIPLES

The goal of a PAPMS is the protection of assets by removing or reducing the exposure of assets to threats and hazards by developing appropriate protective measures. These measures are intended to reduce the likelihood and consequences of a disruptive event, by preventive and preemptive measures and/or effective response measures to recovery to a predetermined level of performance.

An acceptable level of protection is achieved by developing, designing, deploying, and evaluating fit-for-purpose physical asset protection systems. The elements for physical security protection are detailed in Clause 5 and Annex A of this *Standard*. In developing, applying, and improving a PAPMS, decision-makers should apply the following general principles.

4.1 Leadership and Vision

Top management – which refers to the person or persons responsible for decision-making and authorization for executing decisions – establishes the vision, sets objectives, and provides direction and the risk appetite for their organizations. They promote a culture of ownership within the organization where everyone views managing the risks of disruptive events as part of their contribution to achieving the organization's goals and objectives. Top management demonstrates and ensures a commitment to asset protection and effective leadership in the implementation and maintenance of this *Standard*.

4.2 Governance

Physical asset protection (PAP) is viewed as part of an overall good governance strategy. It is part of the organization's philosophy and values, with protection of human life and safety as the primary concern of managing the risks of disruptive events; it is seen as an integral part of organization-wide risk management.

4.3 Needs Oriented

The objectives of the organization are linked to its needs and expectations. Assessing and understanding the organization's assets, needs, and expectations is critical to the success of PAP management. Stakeholder relationships are systematically managed, ensuring a balanced approach between the needs of the organization and other interested parties (e.g., stakeholders, employees, its supply chain, customers, suppliers, financiers, and local and global communities).

4.4 Systems Approach

PAP is a multi-process iterative approach. Identifying, understanding, and managing interrelated processes and elements contribute to the organization's effective and efficient control of its risks. The systems approach examines the linkages and interactions between the elements that compose the entirety of the system. Component parts of a system can best be understood in the context of relationships and interdependencies, rather than in isolation.

4.5 Adaptability and Flexibility

Most organizations operate where the internal and external environments are subject to change, and should conduct ongoing monitoring of the operating environment to identify changes and implement effective change management strategies. Successful organizations are willing to evolve: constantly adapting to reflect the changing operating environment. A PAPMS should be seen as a management framework, rather than a set of activities. As missions, budgets, priorities, and staff continue to change, the structure of the framework will remain predictable – while particular applications vary.

4.6 Managing Uncertainty

PAP management is not always based on predictable threats and quantifiable risks. Estimates and assumptions need to be made in analyzing the likelihood and consequences of threats – both known and unknown – and the vulnerability of the organization and its assets within a changing environment. The management of risk for disruptive events explicitly takes into account uncertainty, especially the nature of that uncertainty and how it should be addressed.

4.7 Physical Assets Protection Perception

It is incumbent upon top management and asset protection professionals to establish a well-defined strategy and communications program to ensure all levels of management and employees understand the goals of the security management system. The PAPMS supports cultural and organizational perception changes. The protection program must be fully understood and supported at the highest level; top management must ensure that all personnel follow the established requirements.

4.8 Convergence of Perspectives

Top management and asset protection professionals need to recognize the relationships and interrelationships between PAP and the other disciplines for managing the risks of events that might

prevent the organization from achieving its objectives. Analysis, planning, implementation, evaluation, documentation, and review activities need to take an organization security risk management perspective, integrating all facets of the functions and processes in the organization. Teaming with other business functions and processes is key to success in protecting the organization's assets.

4.9 *Factual Basis for Decision Making*

The PAPMS supports decision making and outlines the actions that will be taken based on factual analysis, balanced with experience and intuition. A PAPMS increases the ability to review, challenge, and change opinions and decisions. It increases the ability to demonstrate effectiveness of past decisions through reference to data that is accurate, reliable, timely, and in line with the organization's PAP policy.

4.10 *Continual Improvement*

Managers should seek to improve their PAPMS through the measurement, review, and subsequent modification of PAPMS processes, procedures, capabilities, and information. Formal, documented reviews should be conducted regularly. The findings and recommendations of such reviews should be considered by top management, and action taken where necessary.

5. LEADERSHIP AND GOVERNANCE

5.1 *Management Commitment*

Top management shall demonstrate leadership with respect to the security management program by:

- a) Establishing a PAP management policy;
- b) Appointing a person to be responsible for the PAPMS with the authority and competencies to be accountable for the implementation, maintenance, and evaluation of the management system;
- c) Communicating to the organization the importance of meeting PAP management objectives and conforming to the PAPMS policy, its legal obligation, and the need for continual improvement;
- d) Providing sufficient resources and time allocation to establish, implement, operate, monitor, review, maintain, and improve the PAPMS. Resources include people with specialized skills, equipment, internal infrastructure, technology, information, processes, and financial resources;
- e) Setting the risk criteria and appetite; and
- f) Conducting regular management reviews of the PAPMS.

5.2 *Policy*

Top management shall establish and communicate a PAP policy. The policy shall:

- a) Provide a commitment to avoid, prevent, and reduce the likelihood and consequences of disruptive events, including a commitment to human and community safety;
- b) Be consistent with the organization's other policies;
- c) Provide a framework for setting and reviewing PAP objectives, targets, and programs;
- d) Define the organization's requirements for the PAP program; the scope of the physical security applications involved; and the process of implementation, review, and replacement;
- e) Provide a commitment to comply with applicable legal and other requirements to which the organization subscribes;
- f) Be documented, implemented, evaluated, and maintained;
- g) Be communicated to all appropriate people working for or on behalf of the organization;
- h) Be available to appropriate stakeholders;
- i) Be visibly endorsed by top management;
- j) Include a commitment to continual improvement; and
- k) Be reviewed at planned intervals and when significant changes occur to the organization's operating environment.

6. ESTABLISHING THE FRAMEWORK

6.1 General

The organization shall establish, implement, maintain, and improve a PAPMS in accordance with the requirements of this *Standard*. The organization shall continually improve the PAPMS's effectiveness in accordance with the requirements set out in the whole of Section 5 in order to:

- a) Assure the PAPMS can achieve its expected objectives, targets, and programs;
- b) Manage change to the organization's operating environment; and
- c) Identify and address opportunities for improvement.

6.2 Context of the Organization

The organization shall identify and evaluate external and internal factors that are relevant to its purpose and that affect its ability to achieve the expected objectives, targets, and programs of its PAPMS. These factors shall be taken into account when establishing, implementing, and maintaining the organization's PAPMS, as well as addressing priorities.

6.2.1 External Context

The organization shall define and document its external context, including:

- a) The societal, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment;

- b) Infrastructure dependencies;
- c) Supply chain relationships and commitments;
- d) Key issues, threats, and trends that may impact the assets, processes, and/or objectives of the organization; and
- e) Perceptions and values of external stakeholders.

6.2.2 Internal Context

The organization shall define and document its internal context, including:

- a) Assets including its infrastructure, equipment, people, information, reputation, and designs;
- b) Information systems, information flows, and decision making processes – both formal and informal;
- c) Internal stakeholders;
- d) Organizational policies, objectives, and structures (e.g., governance, roles, and accountabilities) for their achievement;
- e) Perceptions, values, and culture; and
- f) Standards and reference models adopted by the organization.

6.2.3 Management Context

The organization shall define and document its risk and resilience management context, including:

- a) Critical assets, activities, functions, services, products, and stakeholder relationships;
- b) The potential impact related to a disruptive incident;
- c) Needs and requirements – including applicable legal requirements;
- d) The organization's overall risk management policy;
- e) The organization's risk appetite or risk aversion;
- f) The nature and types of threats and consequences that can occur to its business and operations;
- g) How likelihood, consequences, and level of risk will be determined; and
- h) How combinations of multiple risks will be taken into account.

6.2.4 Scope of Physical Asset Protection Management System

The organization shall define and retain documented information on the scope of the PAPMS such that its boundaries and applicability can be clearly communicated to internal and external parties.

The organization shall define the boundaries and the scope of its PAPMS, being the whole organization or one or more of its constituent parts. The organization shall:

ANSI/ASIS PAP.1-2012

- a) Establish the requirements for PAP management, considering the organization's mission, goals, internal and external obligations (including those related to stakeholders), and legal responsibilities;
- b) Assign critical operational objectives, assets, functions, services, and products;
- c) Determine risk scenarios – based both on actual and potential internal and external events – that could adversely affect the critical operations, products and functions of the organization; and
- d) Define a scope of the PAPMS in terms appropriate to the size, nature, and complexity of the organization from a perspective of continual improvement.

The organization shall define the scope consistent with protecting and preserving the integrity of the organization and its relationships with stakeholders – including interactions with key suppliers, contractors, outsourcing and supply chain partners, and other stakeholders (e.g., customers, stockholders, the community in which it operates, etc.). Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such processes are controlled.