ASIS INTERNATIONAL

Security Management Standard: Physical Asset Protection

ANSI/ASIS PAP.1-2012

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

ANSI/ASIS PAP.1-2012

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.

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

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

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

Mark Riesinger, CPP, CHS-III, West Bend Mutual Insurance

James Saulnier, CPP, Sprint

Robert Schultheiss, CSC, Risk Decisions

Sarb 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.

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, FSyl, MIExpE, Corp & Executive Solutions Ltd

Tim Hodges, ASIS UK 208

Mike Hurst FIRP, MSyI, Director HJA Fire & Security Recruitment & Hurst Talent Acquisition

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

Sarb Sembhi, CISSP, Incoming Thought

Martin Smith, MBE, The Security Company

Steve Thomas, BP

Simon Oxley, DPhil, Citicus

Steve Wright, PwC

TABLE OF CONTENTS

TABLE OF FIGURES

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:

a) Understanding the organization's context, risk, and PAP requirements;

b) Establishing a policy and objectives to manage risks;

c) Implementing, operating, and maintaining 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 PAPMS; and

e) 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*.

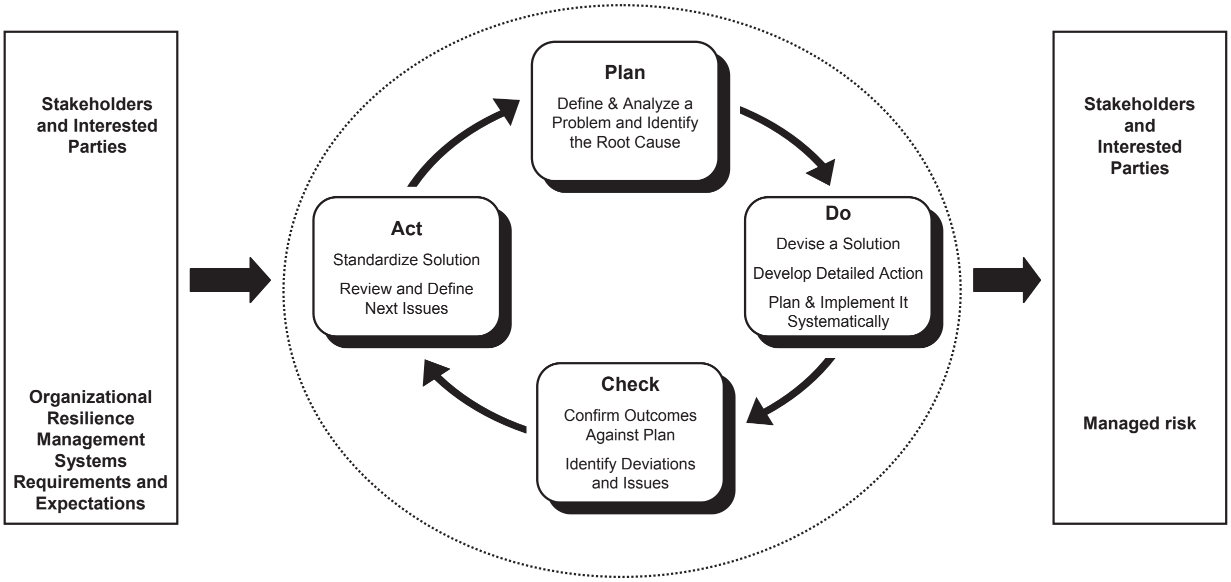
Stakeholders and Interested Parties
Organizational Resilience Management Systems Requirements and Expectations
Plan
Define & Analyze a Problem and Identify the Root Cause
Do
Devise a Solution
Develop Detailed Action
Plan & Implement It Systematically
Check
Confirm Outcomes Against Plan
Identify Deviations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

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.

Annex A
(informative)

A Guidance on the Incorporation of this Standard into the ANSI/ASIS SPC.1-2009, Organizational Resilience Management System Standard

A.1 General

Organizations implementing this *Standard* are required to incorporate the PAP management policy into the ANSI/ASIS SPC.1-2009, Organizational Resilience Standard, or any type of an organization's management system based on the PDCA model. This annex provides informative guidance on incorporating the elements of the PAP management policy. It addresses all the common elements of risk-based management systems using the PDCA model, such as the ANSI/ASIS SPC.1-2009, to enable seamless integration with overall risk and resilience management, as well as more focused policies such as business continuity management. Annex A provides a framework for the organization to manage its security measures to minimize security risks.

It is the organization's responsibility to choose the correct physical security measures and apply them appropriately. Prior to selecting from a range of security measures, a risk assessment should be conducted to focus the application for the measure, consistent with the process described in the ISO 31000:2009, *Risk Management* standard, or as described in the ASIS International *Protection of Assets*. The risk assessment, accompanied by an understanding of practices for physical security measures (provided by this *Standard* used in conjunction with the ASIS International *Protection of Assets* and ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline*), makes it possible for an organization to select and implement appropriate physical security measures to reduce the assessed risks to a level acceptable by the organization.

The PDCA model used in the ANSI/ASIS SPC.1-2009, Organizational Resilience Standard, is illustrated in Figure 2.

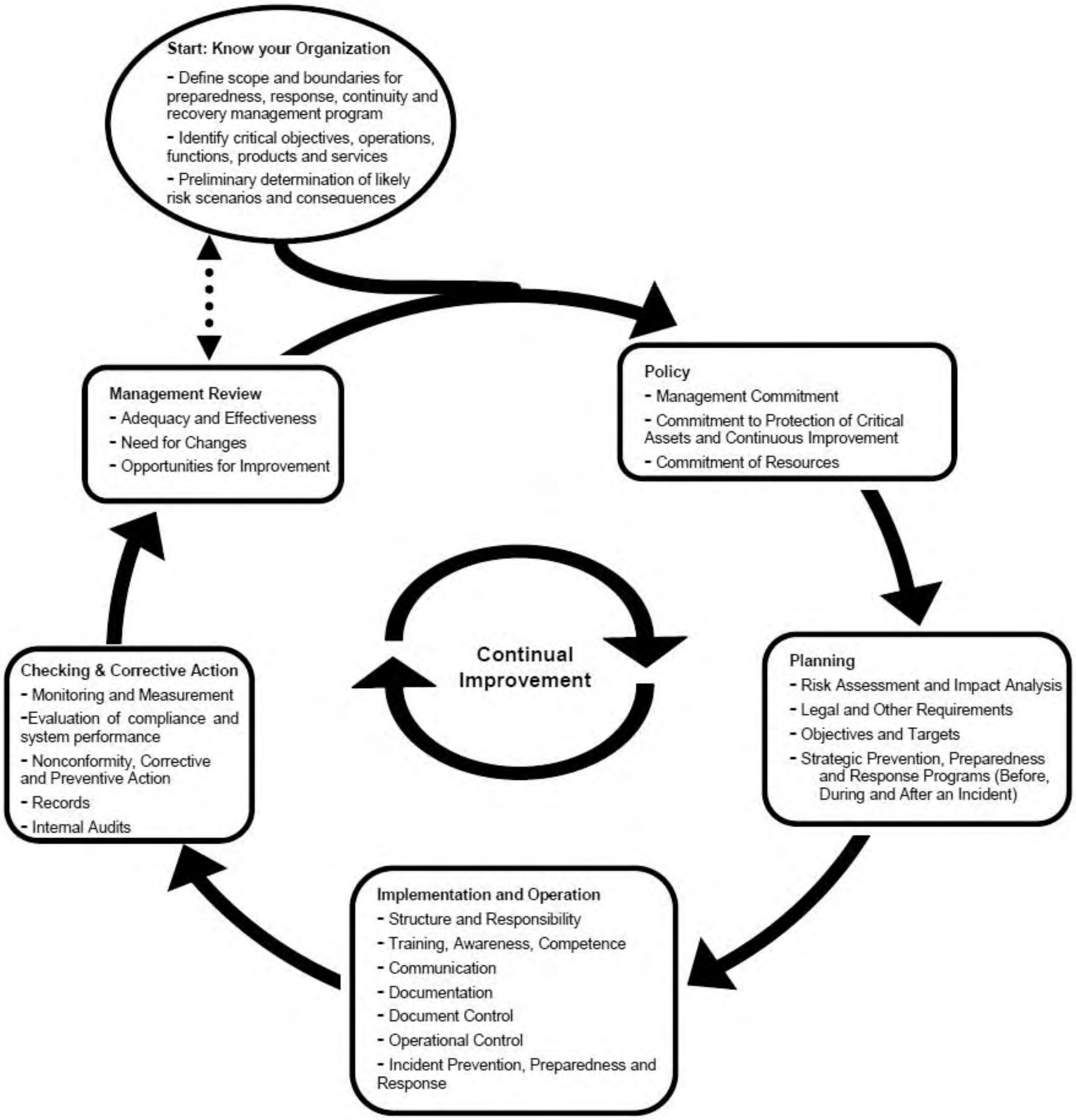
Start: Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences
Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources
Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)
Implementation and Operation
- Structure and Responsibility
- Training, Awareness, Competence
- Communication
- Documentation
- Document Control
- Operational Control
- Incident Prevention, Preparedness and Response
Checking & Corrective Action
- Monitoring and Measurement
-Evaluation of compliance and system performance
- Nonconformity, Corrective and Preventive Action
- Records
- Internal Audits
Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement
Continual Improvement

Figure 2: Organizational Resilience (OR) Management System Flow Diagram

A.2 Support

A.2.1 Resources

The organization should determine and provide the resources needed for the PAPMS, including the design, deployment, maintenance, evaluation, and replacement of PPS.

A.2.2 Communications and Consultations

Communication and consultation with internal and external stakeholders should take place during all stages of the PAPMS process. The organization should establish, implement, and maintain a formal and documented communication and consultation process with internal and external stakeholders to ensure that:

a) Risks and obligations are adequately identified;

b) Interests of stakeholders, as well as interdependencies with internal and external resources and stakeholders, are understood;

c) The PAPMS interfaces with other management disciplines;

d) Needs of internal and external stakeholders are appropriately considered when defining risk criteria and evaluating risks;

e) The design, implementation, and evaluation of PPS are undertaken by qualified and approved PAP professionals;

f) The PAP management process is being conducted within the appropriate internal and external context and parameters relevant to the regional industry standards and codes of practice, the organization, and its stakeholders; and

g) Appropriate and tested means of communication and consultation are available during normal and abnormal conditions.

NOTE: In certain circumstances (e.g., to prevent undue fear or concern or for reasons of informational security), the organization's top management may decide not to communicate sensitive information. In such circumstances, the organization should document the reasons for so doing.

A.3 Documentation

The PAPMS documentation should include:

a) The PAP management policy, objectives, and targets;

b) A description of the scope of the PAPMS;

c) A description of the main elements of the PAPMS and their integration with related documents;

d) Records and documents required by this *Standard*; and

e) Records and documents determined by the organization to be necessary to ensure the effective planning, operation, and control of processes that relate to significant risks.

A.3.1 Records

The organization should establish and maintain records to document conformity to the requirements of its PAPMS, this *Standard*, and the legal and regulatory requirements applicable to the region of application and the results achieved.

A.3.2 Control of Documents

Documents required by the PAP management process and by this *Standard* should be controlled.

The organization should establish, implement, and maintain (a) procedure(s) to:

a) Approve documents for adequacy prior to issue;

b) Review, update, and re-approve documents on a regular basis as well as after an incident or significant operational changes;

c) Ensure that changes and the current revision status of documents are identified and available to appropriate users;

d) Ensure that information of external origin is identified as appropriate, reliable, and controlled;

e) Establish document retention, archival, and destruction parameters;

f) Ensure that original and archival copies of documents, data, and information remain legible and readily identifiable;

g) Ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the PAP management process are identified and their distribution controlled;

h) Identify as obsolete all out-of-date documents that the organization is required to retain; and

i) Ensure the integrity of the documents by ensuring they are tamperproof; securely backed-up; accessible only to authorized personnel; and protected from damage, deterioration, or loss.

The organization should determine the proprietary and security sensitivity of information and should take appropriate steps to prevent unauthorized access.

A.4 Planning

A.4.1 Legal and Other Requirements

The organization should establish, implement, and maintain procedures to:

a) Identify the legal, regulatory, and other requirements to which the organization subscribes related to the threats, hazards, and overall risks to its assets, activities, functions, products, services, stakeholders, environment, and supply chain;

b) Determine how these requirements apply to its threats, hazards, and risks; and

c) Ensure that these requirements are taken into account in establishing, implementing, and maintaining its PAPMS.

The organization should keep this information up-to-date. It should communicate applicable information on legal and other requirements to relevant internal and external stakeholders.

A.4.2 Risk Assessment and Application

The organization should establish, implement, maintain, and update a formal and documented risk assessment process for risk identification, risk analysis, and risk evaluation to systematically assess risk by:

a) Identifying risks due to intentional and unintentional threats that have the potential of direct or indirect consequences on the organization's activities, assets, operations, functions, and stakeholders (threat, vulnerability, and criticality analysis).

b) Analyzing risks to determine those risks that have a significant impact on activities, functions, services, products, supply chain, stakeholder relationships, and the environment (significant risks and impacts).

c) Evaluating and prioritizing risks to determine if they are intolerable, as low as reasonably practical, tolerable, or acceptable:

   a. *Intolerable risks* require treatment at any cost for activities and functions to continue.

   b. *As low as reasonably practical risks* cannot be further reduced without the expenditure of costs disproportionate to benefits.

   c. *Tolerable risks* are negligible or can be managed with routine procedures.

   d. *Acceptable risks* are risks that an organization is prepared to pursue, retain, or take based on informed decision.

d) Selecting, evaluating, and monitoring risk controls and treatments and their related costs and benefits.

To document and keep this information up to date and confidential, the organization should:

a) Continually assess and periodically review whether the PAP management scope, policy, and risk assessment are still appropriate given the organization's internal and external context;

b) Re-evaluate risks within the context of changes inside the organization or its operating environment, procedures, functions, services, partnerships, mutual aid agreements, and supply chains;

c) Re-evaluate risk controls on the outcome of risk events, ensuring a process of investigation, risk treatment, and management acceptance;

d) Evaluate the direct and indirect benefits and costs of options to reduce risk and enhance reliability and resilience to evaluate the cost benefit of treatment options;

e) Ensure that the prioritized risks and impacts are taken into account in establishing, implementing, and operating its PAPMS ; and

f) Evaluate the effectiveness of risk controls and treatments.

The risk assessment and treatment process as described in the ISO 31000:2009 is illustrated in Figure 3.

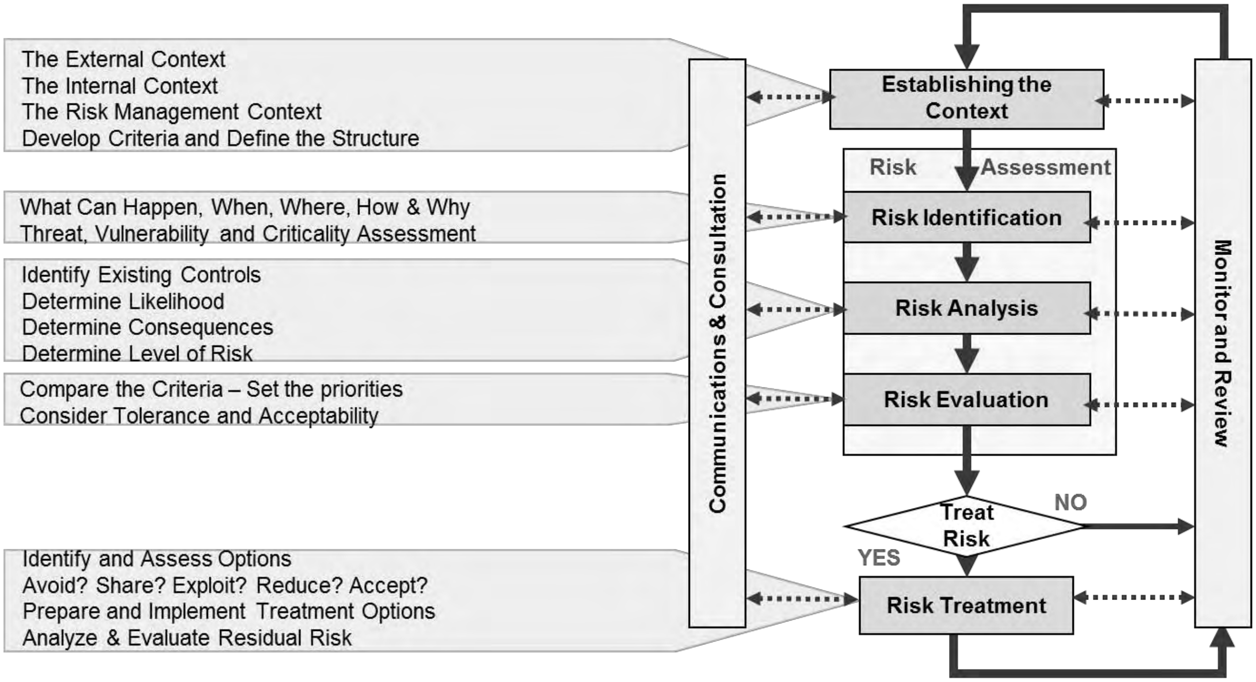
The External Context
The Internal Context
The Risk Management Context
Develop Criteria and Define the Structure
What Can Happen, When, Where, How & Why
Threat, Vulnerability and Criticality Assessment
Identify Existing Controls
Determine Likelihood
Determine Consequences
Determine Level of Risk
Compare the Criteria – Set the priorities
Consider Tolerance and Acceptability
Identify and Assess Options
Avoid? Share? Exploit? Reduce? Accept?
Prepare and Implement Treatment Options
Analyze & Evaluate Residual Risk
Communications & Consultation
Establishing the Context
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Treat Risk
NO
YES
Risk Treatment
Monitor and Review

Figure 3: Risk Assessment and Treatment Process Flow Diagram based on ISO 31000:2009

A.4.2.1 Risk Identification and Exposure

The organization should establish, implement, and maintain a documented security survey procedure to:

a) Identify assets and infrastructures, evaluate existing countermeasures, and the consequences of a malevolent, arbitrary, or unintentional disruptive event;

b) Identify cross-disciplinary and cross-functional interdependencies;

c) Identify and characterize potential adversaries and threat agents; their capabilities, motivations, and tactics; and their likelihood of success;

d) Identify potential targets and their attractiveness;

e) Identify vulnerabilities and estimate the degree of vulnerability in order to identify and evaluate countermeasure options;

f) Identify the requirements for and evaluate the effectiveness of PPS and countermeasures, including operational and performance evaluation;

g) Determine risk scenarios – based both on actual and potential internal and external events – that could adversely affect the assets, operations, and functions of the organization within the context of their potential impact;

h) Report the risks, the processes used to evaluate the risks, and the processes of reporting observations and making recommendations; and

i) Provide the facts for the development, implementation, and continuation of PAP safeguards.

A.4.2.2 Risk Treatment and Selection of Countermeasure Options

The organization should establish, implement, and maintain a formal and documented risk treatment and countermeasure selection process, which should consider:

a) Removing the risk source, where possible;

b) Avoiding the risk by temporarily halting activities that give rise to the risk;

c) Removing or reducing the likelihood of a disruptive event and its consequences;

d) Removing or mitigating harmful consequences;

e) Sharing or transferring the risk with other parties, including risk insurance;

f) Spreading the risk across assets and functions; and

g) Retaining risk by informed decision.

Top management should:

a) Assess the benefits and costs of options to remove, reduce or retain risk;

b) Continually assess and periodically review the risk treatment and countermeasures to reflect changes to the external environment – including legal, regulatory and other requirements – and changes to the organization's policy, facilities, information management system(s), activities, functions, products, services, and supply chain; and

c) Develop and maintain ongoing communication and consultation between internal and external stakeholders.

A.5 Objectives, Targets, and Plans to Achieve Them

A.5.1 Physical Asset Protection Objectives and Targets

The organization should establish, document, implement, and maintain objectives and targets to build a system of PAP within the organization and its supply chain. This can be done by avoiding, accepting, or removing the sources of risk, or by reducing the likelihood or the consequences of risk.

When establishing and reviewing its objectives and targets, the organization should take into account the legal, regulatory, and other requirements to which the organization subscribes. It should also consider its financial, operational and business requirements, human resource and technical capabilities, and the views of interested parties.

Objectives should be derived from and consistent with the PAP policy and risk assessment, providing a basis for selecting one or more controls (e.g., countermeasures) for modifying risks, reducing the likelihood and/or reducing the consequences considering asset value, cost/benefit, and tolerable levels of residual risk. The PAP management objectives should:

a) Determine cost/benefit of different risk control options;

b) Prioritize risk control options and countermeasure needs and requirements;

c) Facilitate opportunities to maintain or improve performance; and

d) Continually monitor, review, and update as appropriate to accommodate change in the risk environment.

Targets should be:

a) Defined at an appropriate level of detail;

b) Specific, measurable, achievable, relevant, and time-based (where practical);

c) Communicated to all relevant staff, employees, and third parties – including contractors and supply chain partners – with the intent that everyone is made aware of his/her individual obligations; and

d) Continually assessed and periodically reviewed to ensure they remain relevant and consistent with the PAPMS objectives and – if necessary – amended accordingly.

A.5.2 Physical Asset Protection Programs (Action Plans to Achieve Objectives)

The organization should establish, implement, and maintain one or more strategic PAP programs for achieving its objectives and targets. The programs should be optimized and prioritized in order to control and treat risks associated with threats, hazards, and impacts of disruptions to the organization and its supply chain. The program(s) should include:

a) Designation of accountability, responsibility, and resources for achieving objectives and targets at relevant functions and levels of the organization;

b) Consideration of its business, operational, and environmental needs; assets, activities, functions, processes; regulatory or legal requirements; contractual obligations; and stakeholders' needs;

c) The means and time-frame by which they are to be achieved;

d) The objectives, design criteria, performance requirements, procurement methods, implementation processes, and lifecycle processes of the PAP systems; and

e) Consistency with organization-wide risk management program criteria and strategy.

The organization should review and evaluate its programs to determine if these measures have provided a cost-effective assets protection solution, introduced new risks, or improved or limited the effect of the physical assets protection systems. The PAPMS programs should be reviewed periodically to ensure that they remain effective and consistent with its objectives and goals. Where necessary, the programs should be amended accordingly.

A.6 Operation and Implementation

A.6.1 Resources, Roles, Responsibility, and Authority for Physical Asset Protection Management

Roles, accountabilities, responsibilities, and authorities should be defined, documented, and communicated in order to facilitate effective PAP management, consistent with the achievement of its PAP management policy, objectives, and programs.

The organization should establish planning, implementation, and evaluation cross-discipline and cross-functional teams with defined roles, appropriate authority, adequate resources (including effective and safe equipment), and rehearsed operational plans and procedures.

Procedures should be established to ensure that fiscal decisions can be expedited, in accordance with established authority levels and accounting principles.

The organization’s designated authority should provide the command and control functions necessary for (a) designated team(s) to enable and support multiple response and recovery plans – triggering them as needed, providing the triage structure required, allocating resources and personnel, and assuring effective direction of the response operations. This would include supporting the organization's business continuity plans and supply chain management protocols as directed by their senior management teams.

A.6.2 Competence, Training, and Awareness

The organization should ensure that people whose job responsibilities provide the potential to prevent, cause, respond to, mitigate, or be affected by significant threats and risks are competent. This competency should be based on education, training, and experience that is appropriate to the assigned role. Documentation of this competency should be retained by the organization.

The organization should identify competencies and training needs associated with PAP management, including the interdependencies of various business functions and processes. It should provide training or take other action to meet these needs, and should retain associated records.

The organization should establish, implement, and maintain controls to ensure that persons doing work on behalf of the organization are aware of:

a) The PAP policy;

b) Their contribution to the effectiveness of the PAPMS, including the benefits of improved PAP performance;

c) The significant threats and risks associated with their work and the benefits of improved personal performance;

d) The procedures to reduce the likelihood and/or consequences of a disruption to the organization;

e) The process of report and referral for further consideration and/or appropriate action by other persons in the organization;

f) The importance of conformity with the PAP management policy and procedures, and with the requirements of the PAPMS;

g) Their roles, accountabilities, and responsibilities in achieving conformity with the requirements of the PAPMS;

h) The effects of their divergence from the PAPMS requirements; and

i) The potential consequences of departure from specified procedures.

A.7 Operational Procedures and Controls

A.7.1 General

The organization should establish, implement, and maintain procedures for countermeasures to prevent and manage its risks that have the potential to harm the organization, its assets, partners, and stakeholders, in order to:

a) Comply with legal and other regulatory requirements;

b) Meet its obligations to its internal and external stakeholders;

c) Deliver its PAP programs (risk treatment and countermeasure action plans); and

d) Achieve its PAP objectives and targets.

The controls should document how the organization will:

a) Provide adequate protection of assets (tangible and intangible), based on the risk assessment;

b) Avoid, remove, or reduce the likelihood of an incident;

c) Reduce and manage the consequences of an incident;

d) Maintain continuity of operations and services;

e) Ensure the integrity of the controls if an incident takes place; and

f) Recover from an incident.

The organization should adopt a “protection in depth” or layered protection strategy to develop a cost-effective and robust approach to deter, delay, detect, deny, respond, and recover from risks and threats to the organization and its assets. The organization should consider layered controls that:

a) Eliminate the risk by complete removal of the risk exposure;

b) Reduce the risk by modifying activities, processes, equipment, or materials;

c) Isolate or separate the assets from risk;

d) Deploy engineering controls to deter, delay, detect, and deny a potential hazard or threat agent;

e) Apply administrative controls such as work practices or procedures that reduce risk; and

f) Provide protection of the asset if the risk cannot be eliminated or reduced.

The value of the asset, the output from the risk assessment, the organization's risk appetite, and the relative cost-benefit of the control measures will determine the number and types of layers needed to adequately protect the asset. Evaluation of interdependencies is critical to a successful protection in depth strategy given the reliance of many physical countermeasures on electronic, telecommunications, and information systems.

A.7.2 Documenting Procedures

The organization should establish, implement, and maintain documented performance criteria and procedures to control situations where their absence could lead to deviation from the PAP policy, objectives, and targets. These procedures should include controls for the design, procurement, installation, operation, maintenance, evaluation, and replacement of PPS as appropriate.

Where existing arrangements are revised and new arrangements introduced that could impact on the PAP management of operations and activities, the organization should consider the associated risks before their implementation.

The operational control procedures should define:

a) Purpose and scope;

b) Objectives and measures of success;

c) Implementation procedures (including phases and sequences);

d) Roles, responsibilities, and authorities;

e) Technology requirements (including maintenance and calibration);

f) Communication requirements and procedures;

g) Internal and external interdependencies and interactions;

h) Resource requirements; and

i) Information flow and documentation processes.

The control procedures should ensure:

a) Demand signals are comprehended in capacity planning;

b) Contingencies and appropriate redundancies provide protection in depth;

c) Processes are in place to validate supplier responses (e.g., validate site/process/product time to recover);

d) There is a feedback loop to know if past risk control and countermeasures are changing as part of design, engineering or process changes, or a decision to outsource certain activities;

e) That planned changes are controlled, and that unintended changes are reviewed and appropriate action is taken; and

f) Procedures are periodically reviewed – and, where necessary – the PPS is revised and documented.

A.7.3 Design of Controls and Countermeasures

The PPS design should be derived from and consistent with the PAP policy and risk assessment necessary to achieve the organization's PAP objectives and targets. It should characterize the organization's functions consistent with the threats to the organization and its vulnerabilities by identifying and integrating the components and elements of the PPS. The organization should design PPS through the process of:

a) Determining the objectives based on the threat, vulnerability, and criticality analyses in the risk assessment to clearly identify threats, vulnerabilities, targets, and potential consequences;

b) Determining cross-functional and cross-disciplinary interdependencies in a team effort;

c) Identifying PPS elements needed to protect assets by reducing the likelihood of a threat successfully materializing, mitigating the consequences should the threat materialize, and planning an appropriate response;

d) Evaluating potential points of failure in the system to determine the appropriate need for redundancies and layered protection methods;

e) Evaluating the competencies required to support effective design and deployment of PPS by qualified, approved, and recognized physical assets protection professionals;

f) Evaluating the systems criteria to develop the design specifications (drawings, schedules, and schematics) for equipment, materials, hardware, and software requirements;

g) Estimating design costs and lifecycle costs, and developing budgets based on evaluation of cost-benefit options;

h) Ensuring a process of acceptance, approval, responsibility, and accountability;

i) Continually monitoring to analyze, assess, measure, and evaluate the effectiveness of the PPS design and design processes; and

j) Maintaining the integrity of the organization and the functions and assets to which the system is to be applied.

The PPS should integrate people, procedures, and equipment for the protection of the organization's assets, its properties, facilities, and operations. The functions of PPS are to deter the occurrence of an undesirable event, delay adversaries from reaching their target, detect an undesirable event or adversary attack, and provide a response to deny adversaries from reaching their target or succeeding in their objective. When designing the PPS, the organization should consider layering the controls and countermeasures, including:

a) Environmental design;

b) Physical barriers and site hardening;

c) Physical entry and access control;

d) Security lighting;

e) Intrusion detection;

f) Video surveillance;

g) Electronic and network controls;

h) Personnel; and

i) Administrative procedures.

The organization should document all phases of the PPS design process.

NOTE: See the ASIS International *Protection of Assets* and the ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline*, for details on design parameters.

A.7.4 Physical Protection Systems Lifecycle

The organization should establish a PPS lifecycle program based on a PDCA model that ensures the continuation of systems objectives, sustainability of the system, integrity of the system, provides evidence of compliance and conformance, and documents all proceedings pertaining to the PPS and the organization's PAPMS. The phases of the PPS lifecycle program are:

a) *Plan*: Based on the risk assessment and objectives, plan the controls and countermeasures:

1. Establish justification of system implementation;
2. Identify the objective and requirements of the system;
3. Determine systems design criteria and design, capacity, and performance requirements;
4. Identify stakeholders and competencies required for the implementation of systems;
5. Identify legal requirements and liability issues; and
6. Develop cost-benefit justification and identify the procurement methods to implement the system.

b) *Do*: Implement the system:

1. Design and deploy the system – including equipment and hardware listings, software, and schedules; design drawings, specifications, and schematics; and information pertaining to the contracting of systems implementation;
2. Provide appropriate training including the provision of operational and response procedures, training manuals, schedules, plans, training agendas, and trainee evaluations;
3. Define operation and maintenance roles and responsibilities; and

   4. Establish a process of systems installations, commissioning, testing, evaluating, acceptance, and rejection.

c) *Check*: Maintain and evaluate system performance:

   1. Establish processes of lifecycle testing, calibration, test data collection and evaluation, warranty plans, reports, records, and upgrade schedules; and

   2. Establish the process of systems maintenance, evaluation, and replacement.

d) *Act*: Change management and continual improvement:

   1. Monitor and evaluate changes to the threat and operational environment;

   2. Implement a process to identify real and potential control and countermeasure shortfalls, and take appropriate corrective and preventive actions; and

   3. Identify opportunities for improvement.

A.7.5 Maintenance, Evaluation, and Replacement

The organization should implement a process of PPS maintenance, evaluation, and replacement to minimize the potential for and impact of systems failures. The organization should:

a) Assign accountabilities and responsibilities to the systems maintenance, evaluation, and replacement processes;

b) Employ both remedial and preventive maintenance services to all components of the PPS;

c) Employ a maintenance program that includes provisions that require demonstrated competent individuals to perform all tests, maintenance, calibrations, and repairs necessary to keep the PPS operational;

d) Develop a system maintenance agreement that denotes the accountabilities and responsibilities of all stakeholders, establishes the organization’s central point of contact, and facilitates agreements between appropriate parties;

e) Regularly review agreements, measure performance, and address the agreement’s scope;

f) Develop and define maintenance service levels that are realistic, objective, measurable, and in accord with the organization’s capabilities;

g) Develop documented maintenance testing programs and a testing schedule with defined periodicity, incorporating a process of reviewing and measuring performance, and resolving non-compliance;

h) Establish and maintain access to a spare parts inventory that minimizes downtime, and develop a process of spare parts purchasing;

i) Develop procedures to identify who is responsible for systems fault identification, problem diagnosis and verification, fault correction, repair testing, repair logging, and maintenance coordination tracking;

j) Keep records and logs of each maintenance task and organize cumulative records for each major component of the system; and

k) Maintain records to demonstrate conformity to the requirements of its PAP systems.

A.7.6 Considerations for Emergency or Unusual Situations and Disruptive Events

The organization should establish, implement, and maintain procedures to prevent, prepare for, and respond to events to ensure the integrity and operability of its PAP system during situations that may have impacts on the organization and its PAP.

The organization should establish, document, and implement procedures for a command and control structure to prevent, prepare for, and manage a disruptive event. This command and control structure should provide for cross-discipline and cross-functional teams with the necessary resources, authority, experience, and competence to:

a) Determine and confirm the nature and extent of a disruptive event, and trigger appropriate control measures;

b) Execute a coordinated response between different business functions and disciplines (e.g., coordination with risk management, information technology, and business continuity teams);

c) Implement plans, processes, and procedures for the activation, operation, coordination, and communication of the prevention, protection, mitigation response, and recovery measures;

d) Communicate with internal and external stakeholders – including supply chain partners, local authorities, and the media; and

e) Evaluate the level of response with the authority to identify actions of each phase of the disruption – including declaring the end of the situation.

It is the responsibility of the organization to develop prevention, preparedness, and response procedures that suit its particular needs. In developing its procedures, the organization should address its needs with regard to:

a) The protection of tangible and intangible assets;

b) The protection of people;

c) The most appropriate methods for mitigation and emergency response to a disruptive event to avoid its escalation to a crisis or disaster;

d) Procedures and authority to assess and declare an emergency situation, activate plans and actions, assess damage, and make financial decisions to assure the continuity of operations;

e) Internal and external communication plans – including notification of appropriate authorities and stakeholders;

f) The actions required to secure physical and information assets;

g) The need for a process for post-event evaluation to establish and implement corrective and preventive actions;

h) Periodic testing of the PPS under normal and abnormal conditions;

i) The potential impact on the PAP system by disruption of critical infrastructure (e.g., electricity, water, communications, transportation) and other dependencies and interdependencies (e.g., information technology systems); and

j) Procedures and actions required to recover the PAP system within the organization's recovery time objective and the resources that it requires for recovery.

The organization should continually assess, and periodically review and revise, its incident prevention, preparedness, and response procedures – in particular, after the occurrence of accidents or incidents that did escalate or could have escalated into an emergency or crisis situation.

The organization should document this information and update it at regular intervals or as changes occur. Incident reports should be included in management review.

A.8 Performance Evaluation

A.8.1 Monitoring and Measurement

The PAP management performance of the organization should be monitored, measured, and analyzed in order to evaluate the effectiveness of the PAPMS.

The organization should establish, implement, and maintain procedures to monitor, measure, and evaluate the effectiveness of PPS and controls including:

a) Operational and performance evaluation, both on a regular basis and after a disruptive event;

b) Communications and information systems; and

c) Projected systems effectiveness to forecast organizational changes.

The procedures should include the documenting of information to monitor the calibration, efficacy, applicable operational controls, PAP management procedures, and conformity with the organization's objectives and goals.

The organization should define:

a) What should be monitored and measured;

b) How and when the monitoring and measuring should be performed;

c) How and when the analysis and evaluation of the results of monitoring and measurement should be performed; and

d) Who should receive these results.

The organization should take appropriate action when necessary to address non-conformance of the PPS.

The organization should keep records of the results of the monitoring and measurement of the PPS.

A.8.2 Evaluation of Compliance

The organization should establish, implement, and maintain procedures for periodically evaluating compliance with legal, regulatory, and other requirements. The organization should take appropriate action when necessary to address non-compliance. The organization should keep records of the results of the evaluations.

A.8.3 Exercises and Testing

The organization should use exercises and other means to test the appropriateness and efficacy of its PAPMS plans, processes, and procedures – including stakeholder relationships and infrastructure interdependencies. Exercises should be designed and conducted in a manner that limits disruption to operations and exposes people, assets, and information to minimum risk.

Exercises should be conducted regularly, after a significant event, following significant changes to the organization's mission and/or structure, or following significant changes to the external environment. A formal report should be written after each exercise. The report should document the formal review of the appropriateness and efficacy of the organization's PAPMS plans, processes, and procedures – including nonconformities – and should propose corrective and preventive action.

Post-exercise reports should form part of top management reviews.

A.8.4 Nonconformities; Corrective and Preventive Action

The organization should establish, implement, and maintain procedures for dealing with nonconformities and for taking corrective and preventive action. The procedures should define requirements for:

a) Identifying and correcting nonconformities and taking actions to mitigate their impacts;

b) Investigating nonconformities, determining their causes, and taking actions in order to avoid their recurrence;

c) Evaluating the need for actions to prevent nonconformities and implementing appropriate actions designed to avoid their occurrence;

d) Assigning accountable and responsible persons to completing each action;

e) Recording the results of corrective and preventive actions taken; and

f) Reviewing the effectiveness of corrective and preventive actions taken.

The organization should ensure that proposed changes are made to the PAPMS documentation. The organization should retain documented evidence of the nature of the nonconformities and any subsequent actions taken to improve performance and their results.

A.8.5 Internal Audit

The organization should establish, implement, and maintain PAPMS procedures to conduct audits at planned intervals and non-periodic basis as determined by top management.

Internal audits should assess whether the PAPMS:

a) Meets the requirements of this *Standard*;

b) Meets the jurisdictional legal and regulatory requirements;

c) Has been properly implemented and maintained; and

d) Has been effective in achieving the organization's PAP management policy and objectives.

Internal audit procedures should:

a) Define responsibilities and requirements for planning and conducting audits, reporting results, and retaining associated records;

b) Define audit criteria, scope, competencies, accountabilities, responsibilities, frequency, and methods;

c) Ensure that the results of the internal audits are reported to the management responsible for the area being audited; and

d) Retain relevant documented information as evidence of the results.

Auditors should be selected and audits should be conducted in a manner which provides objectivity and which demonstrates impartiality of the audit process.

A.9 Management Review

Top management should formally review the organization's PAPMS at planned intervals to ensure its suitability, adequacy, and effectiveness. The reviews should assess opportunities for improvement and the need for changes to the PAPMS, including the policy, scope, objectives, and targets. Records of all top management reviews should be retained.

Input to top management reviews should include:

a) Results of PAPMS audits and routine reviews;

b) Feedback from internal and external stakeholders;

c) Results from exercises and testing;

d) The extent to which objectives and targets have been met;

e) Status of corrective and preventive actions;

f) Follow-up actions from previous top management reviews;

g) Changes in the internal, external, and risk management context of the organization;

h) Changing circumstances, including developments in legal, regulatory, and other requirements; and

i) Opportunities for improvement.

The outputs from top management reviews should include decisions and actions related to possible changes to scope, policy, objectives, targets, and other elements of the PAPMS, with the aim of promoting continuous improvement.

Top management should review the organization's PAPMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.

The organization should:

a) Communicate the outputs of management review to relevant stakeholders;

b) Take appropriate action relating to those outputs; and

c) Retain documented evidence of the results of management reviews.

A.10 Improvement

A.10.1 Maintenance and Change Management

Top management should establish a defined and documented PAPMS maintenance program to ensure that any internal or external changes that impact the organization are reviewed in relation to the PAPMS. The organization should ensure that any necessary changes are made to the PAPMS.

A.10.2 Continual Improvement

The organization should continually improve the effectiveness of the PAPMS through the use of the PAP management policies, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.

Annex B
(informative)

B Informative guidance on the Elements of Physical Asset Protection

B.1 General

This Annex should be used in conjunction with other ASIS International documents that address these topics in greater detail:

- ASIS International, *Protection of Assets*.
- ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline*.

Physical asset protection requires the organization to protect its assets and interests from malevolent acts; undesirable events and changes; the natural, social, and economic environment; and the community in which it and its interests operate. The PAP systems should be implemented, monitored, operated, and tested to deter, delay, and detect with the goal to deny malevolent acts; provide a response to malevolent acts and undesirable events; and provide the processes to recover. The physical security protection systems performance measurements should be aligned and assessed to this.

The PAP systems, their physical applications, and operating procedures should be integrated and aligned to an organization's needs and converged into its overall security and protection systems (such as people, physical, electronic systems, etc.) the functional and operational processes that enforce resiliency and capability to meet changes faced by the organization while protecting its assets. This *Annex* provides the guidelines to implement the individual physical protective measures and PAP applications to the organization's facility, asset, or operation, in conformance to the requirements of the PAPMS.

To achieve the requirements of the PAPMS, PPS should be implemented to provide:

a) *Protection in depth*: The protection system will be implemented to ensure adversaries have to avoid or defeat numerous system components in sequence. This creates additional steps that the adversary must take to defeat the system, requires extensive planning to defeat the system, and reduces the adversary's likelihood to defeat the system. Protection in depth also delays an adversary, thereby providing additional opportunities to detect and respond to an event.

b) *Minimum consequence of component failure*: Instills contingency planning into the protection systems that mitigates against the vulnerability of the systems to component failure and/or the defeat of the protection system.

c) *Balanced protection*: The protection system's individual applications and components will be integrated and converged so that they provide an equal level of protection. Each protection system application or component may be physically or structurally different, but addresses and maintains an adequate level of protection against risks by balancing structural integrity, safety, and costs.

Factors that will influence the adversary's perception of the target fall into a phenomenon referred to by the acronym **CRAVED**[1] whereby assets must be:

a) **C**oncealable;
b) **R**emovable;
c) **A**vailable;
d) **V**aluable;
e) **E**njoyable; and
f) **D**isposable.

The PAP systems should be applied accordingly and conform to the required performance specifications aligned with clearly defined operational requirements – including quantifiable functional monitoring, testing, operating, maintenance, and replacement specifications. Compliance with the performance specifications should be demonstrated upon completion of the installation.

B.1.1 Process of Physical Asset Protection Systems Risk Assessment and Application

The PAP systems should be applied to the organization's facilities, assets, or operations following the risk assessment process outlined in A.4.2, *Risk Assessment and Application*. This will assess and determine the overall risk and the requirements of the PAP system that will be considered to treat the identified risks.

The PAP risk assessment process should be aligned to the overall organizational risk considerations to the facility, asset, or operation where the PAP system is considered for implementation. This should identify the requirements of a single physical asset protection system application, integrated PAP systems implementation, or a fully converged security system that provides a holistic security risk treatment.

B.1.2 Security Survey

The security survey, as part of the risk assessment, is an examination and evaluation of a facility and its policies, procedures, and operations to ascertain its present PAP status, identify deficiencies or excesses, determine the level of protection needed, and make recommendations to improve the overall security of the operation. The security survey is a fact-finding process and is the primary vehicle used in the overall assessment program for the PAPMS. The security surveyor should be able to conduct a comprehensive review, verification, analysis, and appraisal of the organization, its facilities, buildings,

[1] Clarke & Eck. (2005)

assets, and operations by analyzing the facts, drawing conclusions, and making recommendations based on what has been presented.

The objectives of the security survey include:

a) Identifying the scope and assets to be protected;

b) Reviewing the PAP system functionality against its requirement;

c) Identifying critical factors, including interdependencies affecting the security of the facility, asset, or operation;

d) Establishing the continued requirement, and identifying the resources and capabilities, to conform with the continuation of the PAPMS;

e) Reinforcing good practices and encouraging a continuation of those practices in areas of non-compliance;

f) Providing a well written, structured, clear, concise, accurate, and complete survey report; and

g) Providing the basis for performance evaluation.

The organization should:

a) Define the objectives, scope, and outputs of the survey requirements;

b) Employ only accredited (recognized competence) PAP professionals proven in the undertaking and delivery of security surveys;

c) Ensure the surveyor has agreed to and completed contracts, non-disclosure agreements, and due diligence agreements before the survey is undertaken;

d) Ensure the cooperation and availability of all involved persons within the scope of the survey;

e) Make available for review all information, data, documentation, and references as required;

f) Allow access to the organization's facilities, buildings, assets, and areas of operations;

g) Support the security survey, the surveyor, and the requirements to undertake the survey;

h) Regularly review the survey report, monitor, and follow-up on the survey findings, observations, and recommendations; and

i) Reference the survey findings, observations, and recommendations against the applicable risk assessments, and update the risk assessments accordingly.

The security survey could provide the basis for:

a) Developing the security survey into a comprehensive and integrated security analysis and risk assessment across the organization;

b) Identifying the range of potential solutions and their consequences; and

c) Assisting in the development of organization security risk management, continuity, response, and recovery programs.

B.1.3 Cost Benefit Analysis

The organization should introduce and conduct a cost benefit analysis that identifies the costs and benefits of the considered security risk controls and countermeasures to both the individually considered PPS and integrated security systems. Costs and benefits should be measured in terms of effectiveness and efficiency to the accepted levels of risk reduction, avoidance, or acceptance; the reliability of the protection systems to the risk controls; and the time taken to implement the preferred protection system against its alternative solutions. The goal of the cost benefit analysis is to identify the optimal level of risk reduction at the best value available. When conducting a cost benefit analysis, the organization should consider the following:

a) Selection of risk treatments (controls and countermeasures) should be based on the required level of risk reduction and the benefit gained with each risk treatment.

b) Asset value should be compared to the cost of asset loss and production. When determining asset value, it is important to consider the impact of asset loss on production of services or products, asset capability loss, and the cost of lost productivity during the recovery or replacement.

c) Cost benefit analysis is a function of equipment and technology costs, opportunity costs, process impact costs, time costs, personnel costs, and the overall capability costs.

d) Cost benefit analysis is based on risk assessment, and should consider both tangible and intangible assets.

e) When considering combining risk treatment measures, it should consider the trade-offs between design, technology, implementation, maintenance, replacement, training, and administrative solutions by evaluating the costs and benefits of each option (and the order applied).

f) When determining costs, the entire life-cycle of the controls and countermeasures should be considered including:

   a. Design, implementation, and deployment costs.

   b. Purchase price.

   c. Installation and operation costs:

      i. Utility.

      ii. Adaptability, reliability, and scalability.

      iii. Redundancy.

   d. Training costs.

   e. Life expectancy.

   f. Life-cycle maintenance costs.

      i. Preventive maintenance.

      ii. Calibration.

iii. Warranty.

iv. Repair.

v. Replacement.

vi. Disposal.

g) Human resource costs for in-house and external implementation, maintenance, monitoring, and operation.

B.1.4 Security Convergence

Security convergence is a managed process that applies the principles of security risk management to the convergence of individual PAP systems and their integration into an organization's enterprise security systems and enterprise risk management processes. This creates a single managed integrated process aligned to meet the organization's overall security requirements that serves to provide a greater protection against the organization's security risks.

In many organizations, different aspects of security risk management (e.g., PAP, people, information, communications, and continuity management) are managed as separate activities. The recognition of the interdependence of these business functions and processes has led to the development of a more holistic approach to PAP management.

Physical asset protection has become highly dependent on information technology networks, often sharing a common infrastructure and technology platform. Security systems should not be integrated into an organization's computer network unless the organization can clearly secure the systems both physically and technically from intentional or unintentional compromise. Such computerized systems can become the weak point an attacker can exploit to obtain critical information about an organization or disable security systems. Rather than having asset protection and security solutions managed by different business functions applying subjective risk controls to their threat-specific vulnerabilities, convergence provides a common platform where these solutions are assessed and treated from the perspective of a shared risk environment. Information and communications technologies can provide benefits to PPSs (e.g., in implementation, operability, replacement, communications, and overall cost efficiency); however, it may create additional risks and vulnerabilities to the individual and collective systems that should be considered. Security convergence applies a comprehensive and holistic view to the converged security risks – enabling a broad strategic approach that encompasses all areas of security risk – as well as providing for integration with technological advancements.

The ISO/IEC 27001:2005 Standard outlines strategies and controls for information security. It provides a management systems approach and therefore can be used seamlessly with this *Standard*. Likewise, the ANSI/ASIS/BSI BCM.01-2010 Standard can also be used with this *Standard* to manage the consequences of a disruptive event. All of these standards can be applied simultaneously in a single converged management system standard using the ANSI/ASIS SPC.1-2009, *Organizational Resilience Standard*.

The application of security convergence should establish:

a) A cost effective strategy that protects people, information, and property across functions;

b) Governance that ensures top management commitment and allocates ownership and accountability to the converged security risk management program;

c) A cross-discipline and cross-functional risk assessment and management framework that identifies, analyzes, evaluates, and treats all security risks within a singular managed process;

d) A risk management process that monitors all security risks controls and reports weaknesses, vulnerabilities, attacks, and systems failures collectively;

e) A process for ongoing monitoring of changes in communications and information technology risks;

f) Systems that measure and assess the asset protection and PPS performance individually, collectively, and as an entirety of the organization's risk controls;

g) A security risk management framework that functions in synergy with the organization's collective risk considerations;

h) Strategies that coordinate a unified response to disruptive events (attacks), mitigate their consequences, and evaluate and report both the incident and response in order to improve controls to further reduce the likelihood and impacts of an event; and

i) A framework that integrates people, information, technology and procedures.

B.1.5 Crime Prevention Through Environmental Design (CPTED)

Crime Prevention Through Environmental Design (CPTED) is a strategic approach to reducing the risks of malevolent acts and other disruptive events by combining the natural features of a site, the built environment, and the human behaviors associated with a location. This approach uses organizational, mechanical, and natural methods to reduce the likelihood of a threat materializing and/or mitigating its consequences. The CPTED solutions are integrated into the design and functions of facilities.

Facilities and structures (e.g., buildings, parks, garages, and access areas) utilizing CPTED principles can improve the quality of life for people where they live and work by decreasing the opportunity for malevolent acts and increasing the risks to a potential perpetrator.

The CPTED approach focuses on:

a) Manipulating the physical environment to produce behavioral effects that reduce the fear and probability of certain types of malevolent acts and disruptive events;

b) Understanding human behavior in relation to the physical environment;

c) Redesigning space or using it differently to encourage preferred behaviors and discourage illegitimate activities; and

d) Increasing a sense of ownership and territoriality (capable guardian principle).

The level of threat will depend on the intent and capabilities of the adversary. The CPTED approach seeks to diminish the adversary's motivation by reducing his/her confidence of success and lessening the desire to act maliciously. Furthermore, CPTED seeks to increase the resources and knowledge needed by the adversary to succeed in causing a disruptive event. The CPTED approach changes the attributes of the space, thereby altering the adversary's perception of the assets.

There are three general categories of CPTED approaches:

a) *Mechanical measures* emphasize the use of hardware and technology solutions to provide physical protection and discourage the targeting areas where these measures are in place.

b) *Organizational measures* use policies and activities that encourage observation, reporting, and intervention (where appropriate). This includes personnel training for both protection and developing a sense of ownership and responsibility.

c) *Natural* and/or *Architectural measures* incorporate the design and use of space to ensure the overall environment works more effectively for the intended users, while at the same time deterring malevolent and other disruptive events.

The CPTED approach reduces threats by developing and implementing a solution compatible with the designated use of the space while incorporating risk treatment measures intended to minimize both the likelihood and consequences of malevolent acts or other disruptive events. This provides a sense of safety and security for legitimate users.

Typical measures include:

a) Natural access control using physical and symbolic barriers to discourage, prevent access or direct movement to specific access points;

b) Natural surveillance, internally and externally, to increase the capability to detect, deter, delay, and/or respond to potential adversaries;

c) Natural territorial reinforcement/boundary definition to promote a sense of ownership and responsibility;

d) Signage to communicate the designated use of space;

e) Management and maintenance of spaces to look cared for and protected;

f) Activity support to encourage legitimate occupants, residents, customers, or visitors in the desired or intended uses of the space, thereby deterring illegitimate users of the space; and

g) Increasing protection in depth by designing varying layers of public/private uses with well-defined boundaries.

B.1.5.1 Implementation of CPTED

The CPTED process includes:

a) Defining scope of project;

b) Determining the threat environment through research and available data;

c) Working with a multi-disciplinary team to identify needs and concerns;

d) Conducting a risk assessment emphasizing the relationships between the threat, the vulnerability and criticality analysis, and the relevant environmental aspects;

e) Developing and evaluating design plans based on the risk assessment; and

f) Assessing and choosing appropriate CPTED options.

B.1.6 Site Hardening

Providing obstacles to direct, deter, delay, detect, and deny, access to a facility, asset, or operation utilizing both natural and manufactured means is referred to as *site hardening*. The principles of protection in depth should be applied to site hardening and implemented to achieve the overall PAP system objectives. Since most methods can be contravened, a layered approach should include provisions to detect a breach or attempted breach to the protected asset. A delay in depth approach considers the strength of each obstacle to the resources available to an adversary to overcome them. Time afforded by obstacle delays counts toward the overall time for a response to breach.

B.1.6.1 Site Access and Perimeter Delineation

Controlling site access has tangible results when determining measures that support the security in-depth approach; therefore, the site access and perimeter requires delineation. Having a well-defined perimeter eliminates the ambiguity caused by unauthorized access, and clearly indicates intent on the part of the perpetrator. Some sites that are open to the public can still provide site access control by coordinating traffic patterns and separating parking and other vehicular traffic. By limiting the number of access and egress points, surveillance of those points is also easier to maintain. Controlling the quantity and location of parking and deliveries can help manage the risks posed by persons or vehicles that are not thoroughly searched. For example, having a designated parking area for pre-screened vehicles enables resources to be allocated to other areas that pose a higher threat than those in a pre-screened vehicle lot. Separating deliveries from other site traffic allows for easier observation of delivery vehicles and its personnel. Ensuring that site access is controlled (or monitored, at the very least) will increase the depth of protection formed in the PAPMS.

B.1.6.2 Implementation of Site Hardening Systems

The considerations and processes of site hardening should identify the facilities, assets, and operations to be protected; delineate the boundaries and limitations of the protected spaces; and configure a protection system – using the layered approach of protection in depth – surrounding the facility, asset, or operation. The PAP application (such as barriers, entry controls, intruder detection, surveillance, lighting, and manned guarding) required is determined by assigning criticality factors to the facility, asset, or operation – and understanding the impact to the business if the initial PAP system and subsequent restrictive measures are compromised. Individual physical protection applications should be converged with other PAP application and security systems to control access to the site, deter, delay, detect, deny, and respond to a malevolent act, minimizing the impact of a breach and enhancing the success of the overall PAP system.

The psychological deterrence gained through proper site hardening and PAP system implementation by reducing the target attractiveness of a site is also an important benefit to the overall PAP and security system. The following should be considered when considering site hardening and implementing PAP systems:

a) Assess the target attractiveness (design, occupants, local and regional recognition, essential service providers) and threat profile (past, present, and future threats) of the facility, its assets, operations, and the community in which it operates;
b) Assess the overall risks to the site including the vulnerability and accessibility of the site;
c) Evaluate neighboring perimeters and adjacent areas;
d) Formulate a PAP plan and evaluate effectiveness of multiple options of perimeter, outer, and inner security structures – including potential safety issues;
e) Evaluate the cost effectiveness of various options; and
f) Establish response directives and operational procedures for routine inspections, functionality, and breach remediation.

By establishing the overall goals of a site's or facility's PAP and the organization's security requirements, and coordinating and integrating with the other security measures throughout the site, facility or space will substantially increase the measure of security provided by the overall PAP system.

B.2 Security Lighting

Security lighting enables security personnel to maintain a visual assessment capability of assets during the hours of darkness. Security lighting provides the elements of deterrence and detection.

B.2.1 Objectives of Security Lighting

a) There should be high brightness contrast between intruder and backgrounds;

b) Boundaries and approaches should be illuminated;

c) Areas and structures should be illuminated;

d) Lighting levels should meet statutory, regulatory, and standards requirements;

e) Lighting should be integrated with surveillance systems;

f) Color rendition should support video surveillance systems operation;

g) The wiring circuit should be arranged such that a failing lamp does not degrade the overall security plan;

h) There should be minimal time allowance for reactivation of lighting systems after power failures and during disruptive events;

i) There should be back-up lighting, alternative power sources, and redundancies available during a disruption of normal operating conditions;

j) Systems lifecycle costs should be acceptable and aligned to all other security systems costs and implementation programs. Cost considerations include: installation, operation, maintenance, and replacement of the lighting system;

k) Circuits should ideally be protected (e.g., buried);

l) Lighting poles should be robust and have anti tamper covers fitted at the base; and

m) Maintenance programs should ensure operability of lighting system.

B.2.2 Implementation of Security Lighting Systems

a) Lighting should not be used solely as a psychological deterrent. It should be used in conjunction with barrier systems deployed to protect assets;

b) Lighting is relatively inexpensive to maintain and a clear maintenance program should be developed. It should be coordinated with the deployment of technical surveillance systems to ensure areas that need surveillance are suitably illuminated;

c) Security lighting is desirable for all sensitive areas identified through the security risk analysis process that require observation;

d) A secure source of auxiliary power allowing for resilience and redundancy within the system should be installed;

e) Lighting enables security personnel to observe activity around and inside the protected areas of the facility;

f) Lighting improves the ability of security staff to assess visually and intervene on attempts of unauthorized access;

g) Lighting should be integrated with barriers, entry/ access control, and surveillance systems – rather than used as a standalone system; and

h) Consideration should be given to the collateral impacts of the lighting systems (e.g., adjacent property, zoning authorities).

B.3 Barrier Systems

B.3.1 Physical Barrier Systems

A *barrier system* is any type of obstacle provided that causes a direct impact on the speed, time, and tools necessary to circumvent the obstacle. Barriers can be natural site elements, pre-fabricated structural elements, passive, or temporary (deployable). The most cost effective barriers are those that already exist as part of the site, or intended as part of a new site or facility design. Examples of these are storm ponds, drainage ditches, and elevation changes. Utilizing a site's natural flow of traffic (vehicular and/or pedestrian) can locate natural areas of surveillance and allow for an increase in security measures, should the situation warrant it. If a special event or other reason requires a temporary increase in existing security measures, then deployable barriers can be located at pre-determined locations. By incorporating these options into the overall security plan prior to the elevated security need arising, efficiencies in time and effort will result. Depending on the required role of the barrier system, the cost and reliability will need to be ascertained by the PAPMS.

Barriers can provide any or all of the following:

a) Demarcation of the legal boundary of the premises;

b) Channeled entry through a secured area by deterring entry elsewhere along the boundary;

c) A zone for installing intrusion detection, surveillance, lighting systems, and guards;

d) Deterrence of unauthorized people from penetrating a secured area;

e) Forcing an intruder to demonstrate intent to enter the property;

f) Delayed access thereby increasing the possibility of detection and response;

g) Distance (stand-off) between the barrier and the protected area and/or asset;

h) Psychological deterrence;

i) Reduction in the number of security personnel required; and

j) Demonstration of an organization's concern for security.

A barrier's effectiveness is dependent on how much time it can delay an adversary and its ability to detect an unauthorized breach. Effective delay and detection can allow the response time required to prevent an adversary from achieving their final objective. The success of the response in apprehending the adversary is dependent upon the length of time it takes for the response force to become aware of an alarm, assess the situation, and respond. The time of response force awareness is commonly referred to as time of detection. After time of detection, each barrier encountered must provide a delay element in the system to allow the response force to assess the alarm (false alarm, nuisance alarm, intrusion), and provide a response when appropriate to the system design.

B.3.2 Implementation of Barrier Systems

Deploying a physical barrier plan should start with identifying the assets to be protected, delineating the boundaries and limitations of the site, and configuring a barrier system using layers of protection in depth surrounding the asset. The barrier application required is determined by assigning criticality factors to the facility, and understanding the impact to the business if the initial barrier and subsequent restrictive measures are compromised. Barriers should assist other aspects of the security program such as controlling access to the site), and converge with the overall security plan (video surveillance, behavioral analytics, intrusion detection, physical patrols, and general employee security awareness programs) to deter and minimize the impact of a breach and enhance the success of detection and response to a barrier security alert.

The psychological deterrent gained through proper barrier implementation in reducing the target attractiveness of a site is also an important benefit to the overall security scheme. The following should be considered when implementing physical barriers and site hardening:

a) Assess the target attractiveness (design, occupants, local/national recognition, essential service provider) and threat profile (past, present, and possible future threats) of the facility, its assets, operations, and the community in which it operates;

b) Assess the overall risks to the site including the vulnerability and accessibility of the site;

c) Evaluate neighboring perimeters and adjacencies;

d) Formulate a barrier plan and evaluate effectiveness of multiple options of perimeter, and outer and inner security structures – including potential safety issues;

e) Evaluate the cost effectiveness of various options; and

f) Establish response directives and operational procedures for routine inspections, functionality, and breach remediation.

Establishing the overall goals of a site or facility security requirements and coordinating with the other security measures throughout the site, facility, or space will substantially increase the measure of security provided by the overall PAP system.

B.4 Intrusion Detection Systems

Intrusion detection is defined as the detection of a person or vehicle attempting to gain unauthorized entry (directly or remotely) into an area that is being protected by someone who is able to authorize or initiate an appropriate response.[2] An intrusion detection system initiates an early warning to enable a response of an attempted or unauthorized entry into a protected space – or movement of protected property from within a protected space – and provides the protective elements of deterrence, detection, delay, and response.

Intrusion detection systems consist of operators, monitoring devices, sensors, and support equipment. Intrusion detection sensors perform four functions of detection: 1) intruder penetration of a boundary; 2) intrusion motion detection within a protected space; 3) operator validation; and 4) the movement of a protected property within a protected space. They are integrated with barriers, entry control devices, video surveillance systems (video alarm assessment), and alarm communications systems to provide an integrated systems alarm assessment.

Technical components of intrusion detection systems are comprised of three elements:

a) *An alarm sensor*: A device specifically designed to sense and respond to a certain change in its environment conditions;

b) *A circuit or sending device*: A device that transmits the changes in the condition of the alarm sensor to another location where it can be assessed by the specific responder forces; and

[2] Based on Garcia, M. L. (2008)

c) *An enunciator or sounding device*: A device that alerts a change in the alarm condition.

The performance measurements of intrusion detection systems are its probability of intrusion detection, the correct assessment of an intrusion, the sensor device nuisance alarm rate, and the system's vulnerability to defeat.

B.4.1 Objectives of Intrusion Detection Systems

a) Deters an intrusion into or the removal of protected assets from a protected space;

b) Detects an actual or attempted intrusion into a protected space or removal of assets from a protected space;

c) Provides protection in depth to the facilities, buildings, assets, and operations to be protected, enabling a corrective assessment and response; and

d) Meets the needs of the application, integrating with other PAP systems to provide protection in depth to the protected asset and balanced protection to the protected facility, building, asset, or operation.

B.4.2 Implementation of Intrusion Detection Systems

The organization should implement intrusion detection systems based on the application, threats, design criteria, and applicable regulations to the facility, space, or property to be protected. Intrusion detection systems should be designed, installed, and configured as layers of unbroken rings concentrically surrounding the asset to be protected, in correspondence to the delay and response elements of the PAP system. The organization should include:

a) Establishing the parameters and defining the requirements for the implementation of intrusion detection systems to each facility, building, or property to meet its operational objectives;

b) Defining the assets to be protected, the environmental and atmospheric conditions surrounding the asset, the PAP systems to be applied, and the correspondence of the intrusion detection system to these;

c) Designing the intrusion detection system in concentric layers surrounding the asset to be protected with the first layer starting from the outermost layer necessary to provide the furthest delay;

d) Designing the intrusion detection system which ensures consistency to the probability of detection and instills confidence to detect intrusion;

e) Integrating intrusion detection sensors with physical protection barriers, entry control devices, video surveillance, security lighting, and guard force deployments to provide the maximum delay time to the intended target and minimal response time to apprehend the adversary;

f) Establishing operational procedures to reduce false alarms within the system, and enabling corrective responses to activated alarm states; and

g) Deploying contingencies into the intrusion detection system to minimize vulnerabilities that can defeat the system (directly or remotely).

A well-designed intrusion detection system – coordinated with other security measures throughout the site, facility, or space – will enhance the depth of protection for physical assets and provide a solid foundation for the overall PAPMS.

B.5 Physical Entry and Access Control

Entry devices and access control procedures are implemented to monitor and control access of authorized personnel and property into and out of controlled spaces while denying access to unauthorized persons and property. The importance and degree to which monitoring and restriction is needed is determined by analyzing the various requirements predetermined by the nature of the facility, its spaces, and assets to be protected. The application of entry and access controls depends on the level of protection afforded and the proposed need for the controls, which vary to a great degree. Spaces open to the public but restricted by purchasing access (i.e., sporting events, concert venues, amusement parks, etc.) have much different access control requirements than those of a non-public secured facility (i.e., military bases, precious metal storage, prisons, etc.); however, the principles of applying entry devices and access controls remain the same.

Entry control devices and access control procedures should interface with other PAP systems applied to the facility or space to be protected, and should be regularly assessed and audited to meet the requirements of the PAPMS.

B.5.1 Objectives of Entry and Access Control System

Providing an effective access control system requires that several objectives be met. The following is a typical list of those objectives:

a) Permit authorized persons, materials, and/or vehicles access to controlled areas;

b) Detect, minimize, and prevent the access attempts or exit of unauthorized persons, vehicles, or materials from controlled areas;

c) Provide information to the security personnel for the assessment and response to unauthorized entry; and

d) Provide a data audit of who, what, where, and when access to controlled areas has been granted.

These objectives are met by achieving the three fundamental concepts used to identify and verify that a person is authorized to enter a controlled area by:

1. Identifying a valid key or credential – something a person *has*;
2. Validating an identification number or code – something a person *knows*; and

3. Processing the unique characteristic for biometric identification – what *is inherent* to a person.

B.5.2 Implementation of Entry and Access Control Systems

The application of entry control devices must be matched with effective access control procedures. Entry control devices can be used in combinations of two or more technologies (i.e., biometrics and pin code, credential and lock) to enhance the system's level of security. Layers of protection may result in increased verification and throughput times.

The common performance measurements of entry and access control systems are:

a) Throughput: The measure of the time it takes for an authorized person or material to successfully pass an entry or exit point; and

b) False readings and the measure of acceptance.

Entry and access control systems should be designed and installed to provide protection in depth in accordance with the operational requirements with the following considerations:

a) The design, construction, and conditions of the premises – including the modes of operation;

b) The operations being undertaken; the nature, sensitivity, importance, or vulnerabilities of these operations; and the threats directed at these operations and the organization;

c) The area, region, and environment of operations;

d) The value and criticality of the assets to be protected; and

e) The safety, legal, and financial restraints of the entry and access control application.

The organization should:

a) Establish the parameters and define the requirements for the implementation of entry devices and access controls to each facility, space, property, and/or operation;

b) Define the levels of access allowed to defined areas, the entry control systems required to control such access, the procedures required to comply to the access restrictions, and the predetermined levels of controls;

c) Define the processes of access acceptance, access denial, and unauthorized or attempted access responses;

d) Define the processes of material detection, asset handling and control, and adversary detection and response;

e) Ensure entry control components are designed, installed, maintained, monitored, and managed by competent PAP professionals;

f) Install safeguards into the entry and access control systems and devices to protect against attempts to defeat the systems;

g) Ensure PAP personnel are fit for service and required tasks – including the provision of detailed access control procedures implemented to coordinate with the use of entry control devices;

h) Implement a process of frequent, irregular checks or tests of the entry and access control systems and PAP personnel assignments;

i) Establish an identification system where entry into a controlled area is based on the individual being recognized with at least two different forms of the three basic concepts of entry and access control systems;

j) Enforce a uniformed method of wearing and displaying identification credentials for areas of "authorized personnel only";

k) Ensure entry and exit points are constructed to ensure a single file throughput to direct personnel through the control point and to better detect attempts to defeat the controls by unauthorized persons or property;

l) Develop a training and education program for all personnel towards good access control measures aligned to the organization's security and safety policies;

m) Develop a process of issuing, auditing, and invalidating identification credentials; and

n) Clearly define a response to unauthorized access attempts or to personnel attempting to bypass the access control devices.

The access control system will provide some of the most visible security measures which can enhance the deterrent portion of any security scheme. Coordinated with the overall PAPMS, the access control system will be a vital portion of an organization's protection success.

B.6 Video Systems - Video Surveillance

In this age of integrated security, technical and physical systems combine to enable informed assessment of situations undertaken from remote locations. Video surveillance is an assessment tool that can assist in the management of security functions.

Video surveillance systems are meant to be a visual assessment or visual documentation tool. Video surveillance cameras are installed for one (or more) primary reasons:

a) Live surveillance;

b) Post event reconstruction;

c) Deterrence; and

d) Assessment of any alarm activation to determine cause and initiate appropriate response.

B.6.1 Defining Parameters

In order to effectively design and operate a video surveillance system, it is essential to clearly define the following key parameters:

a) *Purpose*: Define the expectations of the system, as they are understood by the team that is evaluating video surveillance as a mitigation system.

b) *Recording duration*: Define what the retention period of video data is expected to be. This may be directed by data protection legislation for the country of operation.

c) *Image quality*: Investigate any local standards that may impact the frame rate, compression, and resolution requirements with regard to image quality and use in legal proceedings.

B.6.2 Systems Architecture

Systems Architecture is a critical issue when dealing with IP-based equipment or multiple location video surveillance systems. Types of architecture include:

a) *Corporate network*: Understand and incorporate information technology for defining the role of the corporate network in supporting the video surveillance system. This coordination should minimally include: Local Area Network use, Wide Area Network use, video client computer use, server equipment and software, switches and routers, anti-virus software and scanning requirements, software updates, equipment firmware updates, internet or external access, priority and latency, and network storage capabilities and requirements.

b) *Security systems/technology network*: If it is determined that the corporate network is inappropriate for use as the primary infrastructure, the previously listed information should be considered as a security system/technology network is developed. Additionally, consideration must be given for access to business network applications (such as e-mail) and any other business systems that are integrated into the design of the video surveillance system.

c) *Stand-alone*: This type of system would be deployed based on a requirement for video equipment at only one site with no additional sites being recommended for inclusion in this project or in the future. Examples of stand-alone systems use may include:

    a. Small business, individual, or isolated locations;

    b. Covert short-term camera placement; and

    c. Organizations which use equipment from multiple sites or facilities with access defined by user level. This introduces a hierarchy of access, with the top tier users being able to see multiple sites, while each site is typically restricted to seeing cameras from their site only.

B.6.3 Signal and Data Transmission

The categories of signal and data transmission are:

a) *Physical point-to-point connectivity (wired or optical)*: Know the different types of image transmission and the cable types and limitations associated with each type of transmission.

b) *Wireless*: Understand the advantages and limitations of wireless video signal transmission and implement accordingly.

The signal transmitted should be on a supervised system. Any loss of signal should generate an alarm signal to the operators.

B.6.4 Recording Methods

It is important to understand the implications of video retention, frame rate, and image quality on data storage. Consideration should be given to "record on motion" versus constant recording (conditional versus linear recording).

a) *Appliance-based*: Typically, a proprietary device located on or within a network infrastructure.

b) *Software-based*: May typically be deployed on company standard computing hardware.

c) *Edge*: Utilizes portable media for processing and recording of images directly at the camera.

B.6.5 System Ownership

System ownerships and responsibility include but are not limited to:

a) *Stakeholders*: Understand and define the stakeholders during implementation, as they may be different from operational stakeholders.

b) *Division of Responsibility*: When developing the stakeholders, define responsibilities for each group. It is important to identify which group is responsible for the different components. This is also a good place to identify service level agreements for each party involved in the operation and maintenance of the system.

B.6.6 Cameras

Video surveillance cameras are selected to provide:

a) Scene identification/general observation;

b) Recognition/action identification; and

c) Personal identification.

There are multiple jurisdictions that have identified general observation categories and requirements. As an example, the following five general observation categories are outlined. These are based on the relative size that a person appears on the viewing screen. The categories are:

1. *Monitor & control*
2. *Detect*
3. *Observe*
4. *Recognize*
5. *Identification*

As an alternative, the ASIS International *Protection of Assets* identifies the categories as:

a) Subject identification;

b) Action identification; and

c) Scene identification.

It is important to understand these concepts and the requirements of the local jurisdiction as the video surveillance system is designed and implemented.

B.6.7 Direct Product Comparisons

It is important in many instances to evaluate the specific pieces of equipment under the conditions of camera placement for compliance with expectations. While specifications of equipment may appear very similar, there are often noticeable differences in image quality based upon many of the aforementioned qualities.

Camera models and features vary widely and are selected by the system designer to meet the needs of the application and scene; they may include:

a) Day/night;

b) Thermal;

c) Analog/IP;

d) Multi streaming; and

e) LPR (License Plate Recognition).

B.6.8 Viewing Clients

Surveillance system video, both live and recorded, can be viewed by one or more of the following methods:

a) Mobile applications;

b) Video walls;

c) Web-based;

d) Computer client (software- based); and

e) Directly from the recording system.

During the design of the system, it is important to identify monitoring requirements, expectations, and capabilities. Each of the above referenced applications has specific requirements and capabilities. It is important to understand the differences and how they impact the design of the system.

B.6.9 System Design

Video surveillance systems should be designed and specified by qualified security and technology professionals. The system designer should include specifications and installation drawings for the needed system components which may include:

a) Camera and lens;

b) Lighting requirements;

c) Equipment mounting details;

d) Recording platform;

e) HVAC requirements;

f) Expansion and scalability;

g) Redundancy;

h) Number of simultaneous users;

i) Signal transmission;

j) Video analytics;

k) Access control and point monitoring;

l) Security operations/command center;

m) Surge protection;

n) Power sources and backup;

o) Documentation requirements;

p) Standardization;

q) Naming conventions;

r) Integration with other business applications;

s) Configuration instructions;

t) Sequence of operations;

u) Testing requirements;

v) Commissioning procedures;

w) Training requirements;

x) Periodic testing; and

y) Specification for routine maintenance and scheduled replacements.

B.6.10 Estimate

Once the requirements are known and the design is complete, the security professional can provide information on the cost of the system. The cost estimate should include costs for:

a) Materials;

b) Installation labor;

c) Software licensing;

d) Training; and

e) Warranty support (Year 1-5).

B.6.11 Procure and Install

With standards-based equipment utilizing the information technology network, there are more options with procurement methods, installation options, and suppliers. The systems are comprised of several specialty disciplines that may include:

a) Voice/data contractor;

b) Server/database professional;

c) Electrical contractor; and

d) Security system integrator.

The stakeholders should identify who will be responsible for the provisioning and support for products needed for the system. Life-cycle cost for system additions, changes, and support should be considered in this phase.

Regardless of the discipline or supplier, each system component should include operation and maintenance manuals with site-specific documentation that provides information on the configuration and settings needed for proper system operation.

B.6.12 Training

Formal training for system users and administrators is needed and most beneficial when they can be trained in the use of their systems. Videos of training classes will provide a consistent way to train new personnel and for review. Training costs can be included or excluded in specification costing.

Training should include:

a) Functional operation of the system;

b) General system architecture;

c) Review of design drawings;

d) Operator commands;

e) Database entry;

f) Backup/restore;

g) Report generation;

h) Alarm assessment;

i) Simple fault finding;

j) System diagnostics;

k) Software/firmware updates; and

l) Alarm response [on site or through an alarm receiving center (ARC)].

B.6.13 Policies and Procedures for System Use

Policies and procedures for systems use should be consistent and conform with:

a) Data protection legislations;

b) National, state, and local laws and regulations;

c) Internal policies/procedures;

d) Industry best practice;

e) Procedures on use of system for internal/external investigations; and

f) Procedures on reporting to outside agencies if system records actions that contravene local laws.

B.6.14 Testing

System testing methods and procedures should be documented and may include:

a) Pre-delivery or factory acceptance;

b) Site acceptance;

c) Reliability or availability tests; and

d) User acceptance testing.

Regardless of the testing method used when the system is accepted, similar tests and system checks will periodically need to be done to maintain the system, to ensure integrity and optimal operation.

B.7 Alarms, Communications, and Display

Collectively, alarms, communications, and display systems work together to form an asset protection system. Electronic data from the alarm system communicates real time data that is filtered, sorted, and prioritized according to local ordinance and end user specification. The product is then displayed at the central monitoring station for human review and response.

B.7.1 Objectives of Alarms, Communications, and Display

The objectives of alarms, communications, and display are to allow for the timely evaluation of information presented by technical systems and any other provider, in an area that provides the capability of responding or coordinating a response based upon the information. An appropriate facility with proper staff, infrastructure, and technology is required to adequately allow for this objective to be recognized.

B.7.2 Implementation of Alarms Monitoring, Communications, and Display Systems

The implementation of an effective command and control center requires consideration and coordination of multiple disciplines. Among the disciplines involved in the design and implementation, consider the following as a minimum:

B.7.2.1 Security

It will be important for the security group to identify the expectations of use of the center.

a) Security measures and accessibility are important to balance when considering location, physical barriers, and technical controls put in place.

b) Identifying the occupants of the center during normal daily activities, as well as users during extraordinary events, is an important part in the success of any center.

B.7.2.2 Technology

It is important to consider the different technical systems that will be incorporated into the center. When reviewing the technical systems that are available for incorporation, it is critical to plan and include adequate infrastructure for the center.

a) *Network infrastructure*: Consider the immediate needs for bandwidth with regard to the existing technical systems to be incorporated. While making this calculation, allow for adequate spare capacity and significant expansion for future capability. Review connectivity requirements with regard to technical systems, business systems, communication systems, the Internet, and any outside support.

b) *Resilience*: When planning the technology to be incorporated into the center, make plans for redundancy of systems, power, communication, and work space. Consider that adding space for another operator during an emergency is considerably easier in the planning and implementation phase than during the response stage.

c) *Space conditioning*: Know that there will be instances that the center may be required to perform under extenuating circumstances with regard to loss of power, connectivity interruption, weather emergencies, and other man-made or natural occurrences.

B.7.2.3 Architectural

The architectural design of the facility should take into account the security and resilience plans when specifying the facility design requirements. Requirements for redundant and emergency power sources, connectivity, and environmental controls are important considerations during the design of facilities. Natural and infrastructure disruptions should be considered in the design phase of facilities.

B.7.2.4 Technical Systems

Utilize technology to the fullest extent possible. Integration of multiple sub-systems should allow improved capabilities for display, monitoring, and response. The use of monitoring by exception should be the standard for implementation. Displaying information that needs to be addressed on the screen focuses the operator's attention to that information. The continual dwell through video images on a monitor does not automatically engage the operator when an exception occurs. The use of technology to evaluate, prioritize, and display the important information greatly enhances the capabilities of the center and the operator.

The information included in this section is intended as a high level guide. It is important to include security professionals in the planning, design, implementation, and operation of this capability.

B.8 Personnel

Personnel play the most significant part in the success of a security program. While multiple technical systems and wide-ranging plans may be implemented to assure security for an organization, these still require the education, cooperation, and involvement of people.

The involvement of people in the security program is related to multiple levels of professionals and everyday users. It should be the objective of any security plan to train, involve, and work with all personnel involved in any facility. It is important to consider, at a minimum, the following classifications of people and their level of involvement:

a) Visitors;

b) Tenants;

c) Employees;

d) Service providers (contractors, delivery, etc.); and

e) Security professionals.

While it is important to include all of this information in any security plan, this section discusses the utilization of security professionals when addressing the security plan.

Physical asset protection measures are typically implemented, monitored, or maintained by security professionals. These personnel range from security managers to security officers and, to varying degrees, all other personnel in the organization. Other ASIS International documents address this topic in greater detail, including:

a) ANS/ASIS CSO.1-2008, *Chief Security Officer (CSO) Organizational Standard*.

b) *Chief Security Officer (CSO) Guideline*.

c) *Private Security Officer (PSO) Selection and Training Guideline*.

It is important to note the four basic options for developing a cost-effective, viable physical security staffing strategy. They include:

1. *Proprietary Security:* This security strategy empowers the company for all security personnel related matters, including hiring and training officers, as well as career enhancements and compensation. This is a traditional business concept for any organization that demands a high level of security, although many organizations have recognized that proprietary security is costly and demands a great deal of corporate resources along with the inherent liability associated with the deployment of a security force.
2. *Contract Security:* The security force is comprised of non-proprietary contract workers hired and supplied by a security provider. In this venue, an organization can save time and money by not recruiting, training, and constantly monitoring the performance of the officers. The security firm also handles all administrative functions – such as uniforms, insurance, and payroll. A contract security firm also can provide a backup pool of officers in the event of an emergency, and eliminate or absorb most overtime costs.
3. *Hybrid Security:* A hybrid team model consists of a combination of proprietary and contract security personnel. This model can help a company retain control of key operations while managing many functions that do not directly affect critical and highly proprietary functionalities. In most cases, it provides flexibility in adapting security needs to specific situations and directly reduces operational expenditures along with some degree of liability. This option focuses on the organization's needs through its modular approach, and helps to ensure expectations are met while affording the greatest level of flexibility.
4. *Total Systems Security Outsourcing:* This approach allows an organization to outsource its total security program, including all security related hardware/software, security officer management and the contract security force itself.

Each scenario must be examined closely and be able to be uniquely tailored to the individual expectations of the organization while maintaining the required level of security. While considering options that include contract providers, it is important to understand the potential differences in jurisdictional requirements. While many authorized jurisdictions provide strict regulation of contract security providers, other areas have no documented requirements for providers to follow. This absence of jurisdictional regulation allows for a large variance in capability, cost, and the level of trust that users should afford contractors. The organization should ensure that all contractors have minimum standards that are agreeable to the organization and meet local regulatory requirements (if any exist).

NOTE: The assistance and approval of the organization’s legal and contract procurement teams should be enlisted before entering into any agreement.

B.9 Security Policies and Procedures

The organization should establish, implement, and maintain procedures to manage the protection of assets. Procedures should be concise and accessible to those responsible for their implementation. Flow charts, diagrams, tables, and lists of actions should be used to complement text.

The purpose and scope of each procedure should be agreed by top management and understood by those responsible for its implementation. Critical interdependencies should be identified, and the relationships between procedures – including those of law enforcement, emergency services, and local authorities – should be stated and understood.

Procedures should describe how the organization will take proactive steps to protect its assets by establishing architectural, administrative, design, operational, and technological approaches to avoid, eliminate, or reduce the likelihood of risks materializing (including the protection of assets from unforeseen threats and hazards), as well as mitigating their consequences.

Organizations may choose to have a single procedure with sections and/or annexes dealing with different types of incident. Alternatively, separate procedures may be written for each type of incident.

Each procedure should specify as a minimum:

a) The purpose and scope of the procedure;

b) Assets to be protected from malevolent or disruptive events;

b) Objectives and measures of success;

c) Implementation steps and the frequency with which the procedure is carried out;

d) Roles, responsibilities, and authorities;

e) Communication requirements and procedures;

f) Internal and external interdependencies and interactions;

g) Resource, competency, and training requirements;

h) Information flow and documentation processes; and

i) Review and revision process.

The organization should nominate a primary "owner" of each procedure and should state who is responsible for reviewing, amending, and updating the procedure. The process of reviewing, amending, updating, and distributing procedures should be controlled.

Annex C
(normative)

C Terms and Definitions

For the purposes of this document, the terms and definitions given in ISO Guide 73:2009 and the following definitions apply:

	Term	Definition
C.1	**access control**	The control of persons, vehicles, and materials through the implementation of security measures for a protected area.
C.2	**alarm system**	Combination of sensors, controls, and annunciators (devices that announce an alarm via sound, light, or other means) arranged to detect and report an intrusion or other emergency.
C.3	**asset**	Anything that has tangible or intangible value to the organization.
C.4	**auditor**	Person with competence to conduct an audit. [ISO 9001:2011]
C.5	**barrier**	A natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials.
C.6	**camera**	Device for capturing visual images, whether still or moving; in security, part of a video surveillance.
C.7	**closed-circuit television (CCTV)**	See *video surveillance*.
C.8	**conformity**	Fulfillment of a requirement.
C.9	**consequence**	Outcome of an event affecting objectives. [ISO Guide 73:2009] NOTE 1: An event can lead to a range of consequences. NOTE 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives. NOTE 3: Consequences can be expressed qualitatively or quantitatively. NOTE 4: Initial consequences can escalate through knock-on effects.
C.10	**continual improvement**	Recurring process of enhancing the PAPMS in order to achieve improvements in overall PAP management performance consistent with the organization's PAP management policy. NOTE: The process need not take place in all areas of activity simultaneously.
C.11	**continuity**	Strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations, and events in order to continue operations at an acceptable predefined level. NOTE: *Continuity*, as used in this *Standard*, is the more general term for operational and business continuity to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for-profit companies, but organizations of all natures, such as non-governmental, public interest, and governmental organizations.
C.12	**contract security**	A business that provides security services, typically the services of security officers, to another entity for compensation.

	Term	Definition
C.13	**corrective action**	Action to eliminate the cause of a detected nonconformity. [ISO 14001:2004]
C.14	**crime**	An act or omission which is in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration; for which a corporation can be penalized by a fine or forfeit; or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts whatever the nature of the penalty.
C.15	**crime prevention through environmental design (CPTED)**	[pronounced *sep-ted*] An approach to reducing crime or security incidents through the strategic design of the built environment typically employing organizational, mechanical, and natural methods to control access, enhance natural surveillance and territoriality, and support legitimate activity.
C.16	**crisis**	An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.
C.17	**critical activity**	Any function or process that is essential for the organization to deliver its products and/or services. [ISO/PAS 22399:2007]
C.18	**criticality analysis**	A process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a disruption on the continuity of the organization.
C.19	**denial**	Frustration of an adversary's attempt to engage in behavior that would constitute an incident.
C.20	**detection**	The act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window, or entering an area without authorization).
C.21	**disruption**	An intentional, unintentional, or natural event that interrupts normal business, functions, operations, or processes, whether anticipated or unanticipated. NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations, or processes.
C.22	**document**	Information and supporting medium. [ISO 9000:2000] NOTE: The medium can be paper, magnetic, electronic or optical computer disc, photography or master sample, or a combination thereof.
C.23	**due diligence**	The care that a prudent person might be expected to exercise in the examination and evaluation of risks.
C.24	**evacuation**	Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas. [ASIS International Business Continuity Guideline: 2005]

	Term	Definition
C.25	**event**	Occurrence or change of a particular set of circumstances. [ISO Guide 73:2009] NOTE 1: Nature, likelihood, and consequence of an event cannot be fully knowable. NOTE 2: An event can be one or more occurrences, and can have several causes. NOTE 3: Likelihood associated with the event can be determined. NOTE 4: An event can consist of a non-concurrence of one or more circumstances. NOTE 5: An event with a consequence is sometimes referred to as "incident".
C.26	**exercises**	Evaluating PAP management programs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g., technology, telephony, administration) to demonstrate PAP management competence and capability. NOTE 1: Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses with the goal of achieving maximum performance. NOTE 2: An exercise can involve invoking response and operational continuity procedures but is more likely to involve the simulation of a response and/or operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise prior to a real invocation.
C.27	**external context**	External environment in which the organization seeks to achieve its objectives. [ISO Guide 73:2009] NOTE: External context can include: • The cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment whether international, national, regional, or local; • Key drivers and trends having impact on the objectives of the organization; and • Relationships with, and perceptions and values of, external stakeholders.
C.28	**facility (infrastructure)**	Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities, and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service.
C.29	**hazard**	Possible source of danger or conditions (physical or operational) that have a capacity to produce a particular type of adverse effect.
C.30	**impact**	Evaluated consequence of a particular outcome.
C.31	**incident**	Event that has the capacity to lead to human, intangible, or physical loss, or a disruption of an organization's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.
C.32	**integrity**	The property of safeguarding the accuracy and completeness of assets. [ISO/IEC 13335-1:2004]
C.33	**internal audit**	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the organization are fulfilled. NOTE: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

	Term	Definition
C.34	**internal context**	Internal environment in which the organization seeks to achieve its objectives. [ISO Guide 73:2009] NOTE: Internal context can include: — Governance, organizational structure, roles, and accountabilities; — Policies, objectives, and the strategies that are in place to achieve them; — The capabilities understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies); — Perceptions and values of internal stakeholders; — Information systems, information flows, and decision-making processes (both formal and informal); — Relationships with, and perceptions and values of, internal stakeholders; — The organization's culture; — Standards, guidelines, and models adopted by the organization; and — Form and extent of contractual relationships.
C.35	**intrusion detection system**	A system that uses a sensor(s) to detect an impending or actual security breach, and to initiate an alarm or notification of the event.
C.36	**lighting**	Degree of illumination; also, equipment, used indoors and outdoors, for increasing illumination (usually measured in lumens, lux, or foot-candle units).
C.37	**likelihood**	Chance of something happening. [ISO Guide 73:2009] NOTE 1: In risk management terminology the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). NOTE 2: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.
C.38	**lock**	A piece of equipment used to prevent undesired opening, typically of an aperture (gate, window, building door, vault door, etc.), while still allowing opening by authorized users.
C.39	**management plan**	Clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the incident management process.
C.40	**mitigation**	Limitation of any negative consequence of a particular incident.
C.41	**nonconformity**	Non-fulfillment of a requirement. [ISO 9000:2005]
C.42	**objective**	Overall goal consistent with the policy that an organization sets itself to achieve. [ISO 14001:2004]

	Term	Definition
C.43	**organization**	Group of people and facilities with an arrangement of responsibilities, authorities, and relationships. NOTE: An organization can be a government or public entity, company, corporation, firm, enterprise, institution, charity, sole trade or association, or parts or combinations thereof.
C.44	**organizational resilience (OR) management**	Systematic and coordinated activities and practices through which an organization manages its operational risks and the associated potential threats and impacts therein.
C.45	**organizational resilience (OR) management program**	Ongoing management and governance process supported by top management resourced to ensure that the necessary steps are taken to: identify the root causes of potential disruptions, likelihood and impact of potential losses; maintain viable adaptive, proactive, and reactive strategies and plans; and ensure stability and sustainability of activities/functions/products/services through planning, exercising, rehearsal, testing, training, maintenance, and assurance.
C.46	**physical protection systems (PPS)**	The integration of people, procedures, equipment, and technology for the protection of assets.
C.47	**physical security**	That part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident.
C.48	**policy**	Overall intentions and direction of an organization as formally expressed by top management.
C.49	**preparedness (readiness)**	Activities, programs, and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies.
C.50	**prevention**	Measures that enable an organization to avoid, preclude, or limit the likelihood and consequences of an event.
C.51	**preventive action**	Action to eliminate the cause of a potential nonconformity. [ISO 14001:2004]
C.52	**procedure**	Specified way to carry out an activity. [ISO 9000:2008] NOTE: Procedures can be documented or not.
C.53	**proprietary security**	Typically, a department within a company that provides security services for that company.
C.54	**protection in depth**	The strategy of forming layers of protection for an asset (see *assets*).
C.55	**record**	Document stating results achieved or providing evidence of activities performed. [ISO 9000:2008]
C.56	**residual risk**	Risk remaining after risk treatment. [ISO Guide 73:2009] NOTE 1: Residual risk can contain unidentified risk. NOTE 2: Residual risk can also be known as "retained risk".
C.57	**resilience**	The adaptive capacity of an organization in a complex and changing environment. NOTE 1: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event. NOTE 2: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.

	Term	Definition
C.58	**resources**	Any asset (human, physical, information, or intangible), facilities, equipment, materials, products, or waste that has potential value and can be used.
C.59	**response and recovery plan**	Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.
C.60	**response and recovery program**	Plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations, and critical assets. [ISO/PAS 22399:2007] NOTE: Response steps generally include incident recognition, notification, assessment, declaration, plan execution, communications, and resources management.
C.61	**risk**	Effect of uncertainty on objectives. [ISO Guide 73:2009] NOTE 1: An effect is a deviation from the expected – positive and/or negative. NOTE 2: Objectives can have different aspects such as financial, health, safety, and environmental goals and can apply at different levels such as strategic, organization-wide, project, product, and process. NOTE 3: Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives. NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances and the associated likelihood of occurrence.
C.62	**risk acceptance**	Informed decision to take a particular risk. [ISO Guide 73:2009] NOTE 1: Risk acceptance can occur without risk treatment or during the process of risk treatment. NOTE 2: Risk acceptance can also be a process. NOTE 3: Risks accepted are subject to monitoring and review.
C.63	**risk analysis**	Process to comprehend the nature of risk and to determine the level of risk. [ISO Guide 73:2009] NOTE: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
C.64	**risk appetite**	Amount and type of risk that an organization is prepared to pursue, retain, or take. [ISO Guide 73:2009]
C.65	**risk assessment**	Overall process of risk identification, risk analysis, and risk evaluation. [ISO Guide 73:2009] NOTE: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.
C.66	**risk criteria**	Terms of reference by which the significance of risk is assessed. [ISO Guide 73:2009] NOTE: Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities, and other inputs to the assessment.
C.67	**risk management**	Coordinated activities to direct and control an organization with regard to risk. [ISO Guide 73:2009] NOTE: Risk management generally includes risk assessment, risk treatment, risk acceptance, and risk communication.

	Term	Definition
C.68	**risk reduction**	Actions taken to lessen the probability, negative consequences, or both, associated with a risk. [ISO Guide 73:2009]
C.69	**risk tolerance**	Organization's readiness to bear the risk after risk treatments in order to achieve its objectives. [ISO Guide 73:2009] NOTE Risk tolerance can be limited by legal or regulatory requirements.
C.70	**risk transfer**	Sharing with another party the burden of loss or benefit or gain for a risk. [ISO Guide 73:2009] NOTE 1: Legal or statutory requirements can limit, prohibit, or mandate the transfer of certain risk. NOTE 2: Risk transfer can be carried out through insurance or other agreements. NOTE 3: Risk transfer can create new risks or modify existing risks. NOTE 4: Relocation of the source is not risk transfer.
C.71	**risk treatment**	Process to modify risk. [ISO Guide 73:2009] NOTE 1: Risk treatment can involve: — Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — Taking or increasing risk in order to pursue an opportunity; — Removing the risk source; — Changing the likelihood; — Changing the consequences; — Sharing the risk with another party or parties [including contracts and risk financing]; and — Retaining the risk by informed choice. NOTE 2: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention", and "risk reduction". NOTE 3: Risk treatment can create new risks or modify existing risks.
C.72	**security**	The condition of being protected against hazards, threats, risks, or loss. NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside. NOTE 2: The term "security" means that something not only is secure but that it has been secured.
C.73	**security aspects**	Those characteristics, elements, or properties which reduce the risk of unintentionally, intentionally, and naturally-caused crises and disasters that disrupt and have consequences on the products and services, operation, critical assets, and continuity of the organization and its stakeholders.
C.74	**security manager**	An employee or contractor with management-level responsibility for the security program of an organization or facility.
C.75	**security measure**	A practice or device designed to protect people and prevent damage to, loss of, or unauthorized access to equipment, facilities, material, and information.
C.76	**security officer**	An individual, in uniform or plain clothes, employed to protect assets.
C.77	**security survey**	A thorough physical examination of a facility and its systems and procedures conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed.

	Term	Definition
C.78	**site hardening**	Implementation of enhancement measures to make a site more difficult to penetrate.
C.79	**source**	Element which alone or in combination has the intrinsic potential to give rise to risk. [ISO Guide 73:2009] NOTE: A risk source can be tangible or intangible.
C.80	**stakeholder (interested party)**	Person or group having an interest in the performance or success of an organization. [ISO/PAS 22399:2007] NOTE: The term includes persons and groups with an interest in an organization, its activities, and its achievements – e.g., customers, clients, partners, employees, shareholders, owners, vendors, the local community, first responders, government agencies, and regulators.
C.81	**stand-off distance/set-back**	The distance between the asset and the threat; typically regarding an explosive threat.
C.82	**supply chain**	The linked set of resources and processes that begins with the acquisition of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user.
C.83	**surveillance**	Observation of a location, activity, or person.
C.84	**target**	Detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives. [ISO 14001:2004]
C.85	**testing**	Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans. [ASIS International Business Continuity Guideline: 2005]
C.86	**threat**	Potential cause of an unwanted incident which may result in harm to individuals, assets, a system or organization, the environment, or the community.
C.87	**throughput**	The average rate of flow of people or vehicles through an access point.
C.88	**top management**	Person or group of people who directs and controls an organization at the highest level. [ISO 9000:2008] NOTE: For example, directors, managers, and officers of an organization who can ensure effective management systems – including financial monitoring and control systems – have been put in place to protect assets, earning capacity, and the reputation of the organization. [ANSI/ASIS SPC.1-2009]
C.89	**video surveillance**	A surveillance system in which a signal is transmitted to monitors/recording, and control equipment. Includes closed-circuit television (CCTV) and network-based video systems.
C.90	**vulnerability**	Intrinsic properties of something that create susceptibility to a source of risk that can lead to a consequence. [ISO Guide 73:2009]
C.91	**vulnerability analysis**	The process of identifying and quantifying vulnerabilities.

Annex D
(informative)

D BIBLIOGRAPHY

ASIS International (2012), *Protection of assets.* Alexandria, VA: ASIS International.

ASIS GDL FPSM-2009, *Facilities Physical Security Measures Guideline.*

ASIS International (2008), *ASIS International glossary of security terms.* [Online]. Available: < http://www.asisonline.org/library/glossary/index.xml > Accessed 2011, August 19.

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

Clarke, R. V., & Eck, J. (2005), *Crime analysis for problem solvers - In 60 Small Steps*. Washington, DC: U.S. Department of Justice. Available < http://www.popcenter.org >

Garcia, M. L. (2008), *The design and evaluation of physical protection systems.* Burlington, MA: Butterworth-Heinemann.

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

ISO 31000:2009, *Risk management – Principles and guidelines.*

Newman (1972) *Defensible space crime prevention through urban design.* New York, NY: Macmillan Publishing Company.

Pearson, R. (2007), *Electronic security systems: A manager's guide to evaluating and selecting system solutions.* Burlington, MA: Elsevier Butterworth-Heinemann.

Tyson, D. (2007), *Security Convergence: Managing Enterprise Risk*. Burlington, MA: Elsevier Butterworth-Heinemann.

ASIS
INTERNATIONAL
Advancing Security Worldwide®

ASIS International (ASIS) is the preeminent organization for security professionals, with 38,000 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, 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, governmental entities, and the general public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management*, ASIS leads the way for advanced and improved security performance. For more information, visit *www.asisonline.org.*

ASIS
INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, Virginia 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

ISBN 978-1-934904-29-9
9 781934 904299