ASIS INTERNATIONAL

Maturity Model for the Phased Implementation of a Quality Assurance Management System for Private Security Service Providers

ANSI/ASIS PSC.3-2013

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

ANSI/ASIS PSC.3-2013

an American National Standard

MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF A QUALITY ASSURANCE MANAGEMENT SYSTEM FOR PRIVATE SECURITY SERVICE PROVIDERS

Approved January 29, 2013

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard* will benefit private security service providers (PSCs) in improving their quality of services consistent with respect for human rights and legal and contractual obligations. It provides a basis for managing risk while reducing costs, demonstrating legal compliance, enhancing stakeholder relations, and meeting client expectations. The model outlines 6 phases ranging from no process in place for quality assurance management, to going beyond the requirements of the *Standard*. Criteria based on core elements of ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations - Requirements with Guidance* can be used to demonstrate continual improvement and are compatible with rewards and recognition programs.

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: 978-1-934904-45-9

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 more than 38,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine – *Security Management* – ASIS leads the way for advanced and improved security performance.

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

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

Commission Members

Charles A. Baley, Farmers Insurance Group, Inc.

Jason L. Brown, Thales Australia

Michael Bouchard, Sterling Global Operations, Inc.

John C. Cholewa III, CPP, Mentor Associates, LLC

Cynthia P. Conlon, CPP, Conlon Consulting 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 PSC.3 Standards Committee, which is responsible for the development of this *Standard*, had the following members:

Committee Members

Committee Chairman: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Committee Secretariat: Susan Carioti, ASIS International

Frank P Amoyaw, LandMark Security Limited
William Badertscher, CPP, Georgetown University
Pradeep Bajaj, Professional Industrial Security Management Academy (PRISMA)
Jonathan Bellish, Oceans Beyond Piracy
Inge Black, CPP, CFE, CPO, CanAm Security Risk Group, LLC
Dennis Blass, CPP, PSP, CFE, CISSP, Children's of Alabama
Anne-Marie Buzatu, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
John Casas, PSP, John Casas & Associates, L.L.C.
Rebecca DeWinter-Schmitt, American University
Bobby Dominguez, CPP, CISSP, PMP, CRISC, GSLC, PSCU Financial Services, Inc.
Jack Dowling, CPP, PSP, JD Security Consultants, LLC
André du Plessis, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Johan du Plooy, CPP, Temi Group
Michael Edgerton, CPP, Good Harbor Consulting, LLC
Thomas Engells, CPP, The University of Texas Medical Branch at Galveston
Glynne Evans, Olive Group Ltd
Windom Fitzgerald, CPP, Pendulum Companies
Stuart Groves, Independent Consultant
Jeffrey Gruber, CPP, CHS-IV, Department of the Army Civilian
Merlin Grue, PSP, Merlin Grue Investigative & Consulting Services
Thomas Haueter, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Lisa Hole, UK Ministry of Defence
Tom Holmes, Edinburgh International
William Imbrie, DynCorp International, LLC
Randy King, DOD Contractors.org, LLC
Christopher Kinsey, King's College London
Mark Knight, Montreux Solutions - Geneva
Mark LaLonde, Canpro Global
Steven Lente, CPP, Securitas Security Services

Tim Lindsey, CPP, Sidwell Protection Services
William Lutz Jr., NICET Level IV, Fire Alarms, Security On-Line Systems, Inc.
Anthony Macisco, CPP, The Densus Group
Christopher Mayer, U.S. Department of Defense
Allan McDougall, PCIP CMAS CISSP CPP, Evolutionary Security Management
Paul Mitchell, GlobalEdge International
Rodney Pettus, The Jones Group
Tracy Philbert, Plexus Consultancy
Werner Preining, CPP, CMAS, Interpool Security Ltd
William Prentice, Marine Security Initiatives, Inc.
Daniel Puente Pérez, Sociedad de Prevención de Asepeyo
Erik Quist, EOD Technology, Inc. (EODT)
Ian Ralby, I.R. Consilium
Eric Rojo, Magination Consulting International
Maya Siegel, SEMSI
Matt Silcox, CPP
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.
Teresa Stanford, CPP, Security Engineers, Inc.
Barry Stanford, CPP, AEG
Timothy Sutton, CPP, CHSS, Securitas Security Services
Roger Sylvester, CPP, Ensign-Bickford Industries
Karim Vellani, CPP, Threat Analysis Group, LLC
Erika Voss, CBCP, CORM, MBCI, Amazon
Colin Walker, Mclean Walker Security Risk Management Inc.
Roger Warwick, CPP, UNI
Eric Davoine
Dale Wunderlich, CPP, A. Dale Wunderlich & Associates, Inc.

Working Group Members

Working Group Co-chairmen:

Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Ian Ralby, Ph.D., Executive Director, I.R. Consilium

Frank P Amoyaw, LandMark Security Limited
William Badertscher, CPP, Georgetown University
Pradeep Bajaj, Professional Industrial Security Management Academy (PRISMA)
Dennis Blass, CPP, PSP, CFE, CISSP, Children's of Alabama
John Casas, PSP, John Casas & Associates, L.L.C.
André du Plessis, DCAF
Johan du Plooy, CPP, Temi Group
Glynne Evans, Olive Group Ltd
Jeffrey Gruber, CPP, CHS-IV, Department of the Army Civilian

Lisa Hole, UK Ministry of Defence (representing UK Government)
Mark Knight, Montreux Solutions - Geneva
Steven Lente, CPP, Securitas Security Services
Tim Lindsey, CPP, Sidwell Protection Services
Anthony Macisco, CPP, The Densus Group
Christopher Mayer, Department of Defense
Allan McDougall, PCIP CMAS CISSP CPP, Evolutionary Security Management
Ian Ralby, I.R. Consilium
Maya Siegel, SEMSI
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.

Table of Contents

0. INTRODUCTION IX

0.1 General IX
0.2 Human Rights Protection X
0.3 Management Systems Approach XI

1. SCOPE OF STANDARD 1

2. NORMATIVE REFERENCES 1

3. TERMS AND DEFINITIONS 2

4. MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF ANSI/ASIS PSC.1-2012 4

4.1 Maturity Model 4
4.1.1 What is a Maturity Model? 4
4.1.2 Why Use a Maturity Model? 4
4.1.3 Using a Maturity Model with the Management Systems Approach. 5
4.2 Phases of the Maturity Model 6
4.2.1 Phase One – Pre-awareness 6
4.2.2 Phase Two – Project Approach 7
4.2.3 Phase Three – Program Approach 7
4.2.4 Phase Four – Systems Approach 8
4.2.5 Phase Five – Management System 8
4.2.6 Phase Six – Holistic Management 9
4.3. Maturity Model Matrix (Management Systems Approach) 9

A. USING THE MATURITY MODEL IN AN INTERNAL RECOGNITION PROGRAM 34

B. GETTING STARTED USING THE ANSI/ASIS PSC.1-2012 35

C. REFERENCES 38

Table of Figures

Figure B.1 : Upward spiral implementation of the standard (based on the PDCA Model) 37

Table of Tables

Table 1: Maturity Model for the Phased Implementation of the ANSI/ASIS PSC.1-2012 Quality Assurance Standard ... 11

This page intentionally left blank.

0. Introduction

0.1 General

The Quality Assurance Maturity Model is a methodology designed to help Private Security Service Providers including Private Security Companies (collectively "PSCs") implement a Quality Assurance Management System (QAMS) consistent with respect for human rights, legal obligations, and good quality assurance practices. This maturity model (referred to here as the *Standard*) for the phased implementation of the ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations – Requirements with Guidance* quality assurance standard (referred to here as the "standard"), may be used by any type of PSC regardless of their size, scope, or complexity; particularly those operating in circumstances of weakened governance where the rule of law has been undermined due to human or naturally caused events. The *Standard* accommodates diverse jurisdictional, geographical, cultural, operational, and social environments.

Adopting a process for the phased implementation of a QAMS ("maturity model") helps the organization determine how to manage change and cost-effectively address the uncertainty in achieving its objectives. The purpose of this *Standard* is to improve and demonstrate consistent and predictable quality of services provided by PSCs while maintaining the safety and security of their operations and clients within a framework that aims to ensure respect for human rights, national and international laws, and fundamental freedoms. Given the finite resources of organizations, it is imperative that they have tools to address the array of threats, hazards, and risks they may face. The maturity model described in this *Standard* helps organizations establish, implement, and maintain a QAMS (e.g., ANSI/ASIS PSC.1-2012) to better manage the risks of potentially undesirable and disruptive events through anticipation, assessment, prevention, protection, mitigation, response, and recovery.

Throughout this *Standard*, reference is made to managing risks. PSCs inherently operate in high risk environments. The organization needs not only to manage risks related to its operations and internal stakeholders, but also those related to external stakeholders upon whom the organization impacts and who can impact the organization. Therefore, the organization must also consider the risks related to its clients, as well as impacted communities. Sources of risk include, but are not exclusive to: legal, security, safety, human resources, cultural, environmental, financial, socio-political, and operational factors. In order to provide a quality of service while demonstrating respect for human life and rights and in order to fulfill contractual obligations, the organization should strive to proactively treat risks minimizing the likelihood and consequences of undesirable and disruptive events. Risk management objectives need to support the organization's quality assurance management objectives.

This *Standard* identifies six phases of maturity to achieve continual improvement of quality assurance through a management framework. The maturity model helps organizations achieve the benefits of quality assurance management by "phasing in" a system tied to the organization's business needs and economic realities, emphasizing a priority to protect life and

respect human rights, national and international laws, and fundamental freedoms. The maturity model enhances an organization's capacity to manage quality assurance to better prevent when possible, mitigate, respond to, and recover from undesirable and disruptive events. The body of this document provides criteria to plan, do, check, and act, in order to drive continual improvement of the management system.

This model outlines six phases of implementation of ANSI/ASIS PSC.1-2012, ranging from a pre-awareness phase (no process in place for quality assurance management) to holistic management (going beyond the requirements of ANSI/ASIS PSC.1-2012), to promote quality assurance management with stakeholders. Using this maturity model, an organization can achieve and maintain an appropriate level of quality assurance management with respect for legal obligations and human rights as part of an organization's culture.

The maturity model for the phased implementation of ANSI/ASIS PSC.1-2012 is a series of steps designed to help organizations evaluate where they currently are with regard to quality assurance management, create a business case for a QAMS, establish goals for achievement, benchmark where they are relative to those goals, and plot a business-sensible path to attain conformance with ANSI/ASIS PSC.1-2012. Standards are designed to promote managed and repeatable performance. Managed and repeatable performance will be achieved by moving to a level appropriate for the organization with the goal being to achieve full conformance with ANSI/ASIS PSC.1-2012 and going beyond conformance to the sixth step whenever possible.

This *Standard* is designed so that it can be integrated with quality, safety, environmental, information security, risk, resilience, and other management systems within an organization. A suitably designed maturity model for phased implementation can thus satisfy the requirements of other management systems standards. Organizations that have adopted a management system (e.g., according to ANSI/ASIS SPC.1-2009, ISO 9001:2000, ISO 14001:2004, ISO 28000:2005, and/or ISO/IEC 27001:2005) are encouraged to use this *Standard* in conjunction with their existing management systems.

0.2 Human Rights Protection

While states and their entities must respect, uphold, and protect human rights, all segments of society (public, private, and not-for-profit) have a shared responsibility to act in a way that respects and does not negatively impact upon human rights and fundamental freedoms. States, clients, and PSCs have a shared responsibility to establish policies and controls to assure conformance with the legal obligations and recommended good practices of the *Montreux Document* and *International Code of Conduct* (ICoC). Organizations, regardless of their level of maturity, have an obligation to respect human rights in all of their operations and activities.

The PSC.1 standard emphasizes the sanctity of life of all stakeholders, therefore:

- At the most basic "Pre-Awareness" level, organizations may not knowingly do anything that would adversely affect the human rights of persons working on their behalf, clients and other persons they are contracted to protect, or local communities and the general population in their theatre of operation. However, from the Project Approach (Phase 2)

onwards organizations assess the human rights risks associated with their operations and take appropriate actions;

- Starting with the second phase of the six phase maturity model, organizations should establish and communicate a policy describing top management's commitment to the respect for human rights and the importance of incorporating that respect into the organization's operations and procedures;
- As organizations mature, they will identify and assess human rights risks associated with their operations, and develop risk treatment strategies; beginning with individual projects and maturing to encompass organization-wide activities;
- An awareness of the need to proactively manage risks that may result in undesirable and disruptive events and respect human rights increases with each phase of maturity. Organizations move from merely reacting to events as they occur to anticipating the potential for events and initiating pre-emptive measure to minimize their likelihood;
- As organizations mature, they establish proactive mechanisms to address undesirable and disruptive events to manage incidents in order to mitigate their impacts, as well as establish methods for the reporting, investigation and remediation of incidents; and
- Continual improvement drives a commitment to respect and promote human rights as inseparable from the provision of security services, by all personnel at all levels of the organization.

0.3 Management Systems Approach

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to minimizing the risks of potentially undesirable and disruptive events. A management system provides the framework for continual improvement to increase the likelihood of enhancing the quality of services while assuring the protection of human rights and fundamental freedoms. It provides confidence to both the organization and its clients that the organization is able to manage its safety, security, and legal obligations while clearly demonstrating the integration of the respect for human rights into its activities and operations.

Through the full implementation, ongoing maintenance, and continual improvement of the ANSI/ASIS PSC.1-2012 quality assurance management system, an organization is able to reach the ultimate goal of ensuring quality assurance consistent with respect for human rights, legal obligations, and good practices. The phased approach recognizes that the QAMS must be aligned with the organization's needs, resources, capabilities, and constraints in order to support continual improvement.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources that are 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 considers how local policies, culture, actions, or changes influence the state of the organization as a whole and its environment. The component parts of a system can best be understood in the context of relationships with each other, rather than in isolation. Therefore, a management system

examines the linkages and interactions between the elements that compose the entirety of the system. The management systems approach systematically defines activities necessary to obtain desired results and establishes clear responsibility and accountability for managing key activities.

The maturity model approach for a QAMS presented in this *Standard* encourages its users to emphasize the importance of:

a) Understanding an organization's internal and external context, risk, as well as human rights and legal obligations;
b) Establishing a policy and objectives to manage risks;
c) Implementing and operating controls to manage an organization's risk and security requirements while respecting human rights;
d) Monitoring and reviewing the performance and effectiveness of the QAMS, administratively and operationally; and
e) Continual improvement based on objective measurement.

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

1. **Phase One:** *Pre-awareness* – Ad hoc quality assurance activities, no process currently in place, and quality assurance management is absent with no advanced preparation. Top management does not recognize the benefits of quality assurance management.
2. **Phase Two:** *Project Approach* – Commonly known as "the awareness phase", where management is willing to test the concept and establish a trial project to explore the benefits of quality assurance management consistent with respect for human rights, legal obligations and good practices.
3. **Phase Three:** *Program Approach* – An expansion of the project approach. The organizational view begins to shift from specific issues to addressing division- or organization-wide issues implementing the core elements of the base standard.
4. **Phase Four:** *Systems Approach* – This phase involves integrating the core elements of ANSI/ASIS PSC.1-2012. Proactive quality assurance management is viewed as part of an iterative continual improvement process using the Plan-Do-Check-Act (PDCA) model.
5. **Phase Five:** *Management System* – All the core elements of the base standard have been applied, evaluated and validated for bringing the organization into full conformance with ANSI/ASIS PSC.1-2012.
6. **Phase Six:** *Holistic Management* – Quality assurance management culture is well-developed and is considered an inseparable part of decision making.

The six phases of the model are focused on the phased implementation of a management system standard, all of which are applicable to any discipline or type of management system that seeks to treat risk. In the maturity model's application to the QAMS, the phases move from reaction to events to addressing known issues mitigating consequences, to balanced and preemptive strategies for anticipation, assessment, prevention, protection, preparedness, mitigation, and response and recovery appropriate to minimizing the likelihood and consequences of undesirable and disruptive events.

Maturity Model for the Phased Implementation of a Quality Assurance Management System for Private Security Service Providers

1. Scope of Standard

This *Standard* provides guidance for the use of a maturity model for phased implementation of ANSI/ASIS PSC.1-2012 as a series of steps designed to help organizations:

- Evaluate where they currently are with regard to quality assurance management consistent with respect for human rights, legal obligations, and good practices.
- Set goals for where they want to go, and benchmark where they are relative to those goals.
- Plot a business/mission appropriate path to get there.

The model outlines six phases ranging from an unplanned approach to managing events, to going beyond the requirements of the *Standard*, and creating a holistic environment for quality assurance management.

2. Normative References

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

a) ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations - Requirements with Guidance* [1]
b) *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict*, U.N. doc. A/63/467-S/2008/636 (2008).)[2]; and
c) *International Code of Conduct for Private Security Service Providers* (ICoC) (11/2010)[3].

[1] This document is available at https://www.asisonline.org/guidelines/published.htm.

[2] For the most current version, go to: http://www.eda.admin.ch/psc.

[3] This document is currently available at http://www.icoc-psp.org.