ASIS INTERNATIONAL

Quality Assurance and Security Management for Private Security Companies Operating at Sea - Guidance

ANSI/ASIS PSC.4-2013

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

ANSI/ASIS PSC.4-2013

an American National Standard

QUALITY ASSURANCE AND SECURITY MANAGEMENT FOR PRIVATE SECURITY COMPANIES OPERATING AT SEA – GUIDANCE

A management systems approach for maritime private security service providers operating at sea

Approved January 29, 2013

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard* provides guidance for the implementation of the ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations - Requirements with Guidance* and/or the ISO 9001:2008, *Quality management systems – Requirements* or the ISO 28000:2007, *Specification for security management systems for the supply chain* standards. The guidance enables Private Maritime Security Companies (PMSCs) to implement these management systems which contain auditable criteria for private security company operations at sea. This *Standard* enables organizations operating at sea to implement the auditable requirements of the ANSI/ASIS PSC.1 and/or the ISO 9001 or ISO 28000 based on the Plan-Do-Check-Act model for third-party certification of PMSCs working for any client.

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 should not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-934904-46-6

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 (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

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.4 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 Amoyaw, LandMark Security Limited
Deborah Avant, Consultant
Jonathan Bellish, Consultant
Brian Bewley, Tactical Solutions International, Inc.
Dennis Blass, CPP, PSP, Children's of Alabama
Michael Bouchard, CPP, Security Dynamics Group LLC
James Browning, Consultant
Anne-Marie Buzatu, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Phillip Cable, Maritime Asset Security and Training
Sékou Camara, Ministry of Foreign Affairs
John Casas, PSP, John Casas & Associates, L.L.C.
Stuart Casey-Maslen, Geneva Academy of International Humanitarian Law and Human Rights
Ioannis Chapsos, Centre for Peace and Reconciliation Studies (CPRS)
Andrew Clapham, Geneva Academy of International Humanitarian Law and Human Rights
Eric Davoine, Consultant
Renee de Nevers, Maxwell School, Syracuse University
Bill DeWitt, CPP, SSA Marine, Inc.
Bobby Dominguez, CPP, CISSP, PMP, CRISC, GSLC, PSCU Financial Services, Inc.
Debborah Donnelly, International Association of Maritime Security Professionals (IAMSP)
Jack Dowling, CPP, PSP, JD Security Consultants, LLC
Tanawah Downing, CPP, PSP, PMP, Global Government Services
André du Plessis, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Johan Du Plooy, CPP, Temi Group
Lisa DuBrock, CPA, CBCP, MBCI, RABQSA-RES, Radian Compliance, LLC
Michael Edgerton, CPP, Good Harbour International
Glynne Evans, Ph.D., Olive Group Ltd
Dimitris Fakiolas, Consultant
Richard Ferraro, Centanni Maritime, Inc.
Windom Fitzgerald, Fitzgerald Technology Group
Bruce Gray, Hornsby de Gray

Laura Hains, CPP, Consultant
Stuart Hattersley, Consultant
Thomas Haueter, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Alan Hunter, Centre for Peace and Reconciliation Studies
Mark Knight, Montreux Solutions Geneva
Timothy Lindsey, CPP, Sidwell Protection Services
Anthony Macisco, CPP, The Densus Group
Duncan MacLeod, CPP, Battelle Memorial Institute
Nick Maroukis, Triton Risk MSS
Paul McCarthy, Consultant
Allan McDougall, PCIP, CMAS, CISSP, CPP, CSO, PFSO, SSO, Evolutionary Security Management
Oona Muirhead, Security in Complex Environments Group, ADS UK
Vicki Nichols, RABQSA-RES, Consultant
Henri Nolin, CPP, Sun State Specialty K9S Inc.
Rodney Pettus, The Jones Group
Russ Phillips, MMTS Group
Werner Preining, CPP, CMAS, Interpool Security Ltd
William Prentice, Marine Security Initiatives, Inc.
Erik Quist, EOD Technology, Inc. (EODT)
Ian Ralby, Ph.D., I.R. Consilium
James Rapp, 3rg Security
David Reindrop, Ministry of Defence
Chris Rossis, Argonaut Security LTD
Michael Segkos, Sea Guardian (SG) Ltd.
Samantha Sheridan, Triton International Ltd
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.
Leslie Smith, Securewest International
J. Stewart, Intelsat
Laurie Thomas, University of Findlay
Jonathan Tipton, Triskelion
Ilijana Todorovic, Consultant
Lloyd Uliana, Bosch Security Systems, Inc.
Roger Warwick, CPP, UNI
Jerry Williams, Aegis Defence Services Ltd

Working Group Members

Working Group Co-Chairs:

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

Co-Chair: Ian Ralby, Ph.D., I.R. Consilium

Frank Amoyaw, LandMark Security Limited

Dennis Blass, CPP, PSP, Children's of Alabama
Michael Bouchard, CPP, Security Dynamics Group LLC
John Casas, PSP, John Casas & Associates, L.L.C.
Bill DeWitt, CPP, SSA Marine, Inc.
Michael Edgerton, CPP, Good Harbour International
Glynne Evans, Ph.D, Olive Group Ltd
Windom Fitzgerald, Fitzgerald Technology Group
Stuart Hattersley, Consultant
Mark Knight, Montreux Solutions Geneva
Anthony Macisco, CPP, The Densus Group
Duncan MacLeod, CPP, Battelle Memorial Institute
Allan McDougall, PCIP, CMAS, CISSP, CPP, CSO, PFSO, SSO, Evolutionary Security Management
Russ Phillips, MMTS Group
Werner Preining, CPP, CMAS, Interpool Security Ltd
Erik Quist, EOD Technology, Inc. (EODT)
Ian Ralby, Ph.D., I.R. Consilium
James Rapp, 3rg Security
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.
Laurie Thomas, University of Findlay
Jonathan Tipton, Triskelion

TABLE OF CONTENTS

Table of Figures

This page intentionally left blank.

0. INTRODUCTION

0.1 General

Crime and piracy at sea has become a global menace that threatens not only international trade but the delivery of vital humanitarian aid to people affected by natural and manmade disasters. Maritime Private Security Service Providers including Private Maritime Security Companies (collectively "PMSCs") are playing an important role in protecting sea-bound assets in conjunction with the public and private sectors[1]. Ships at sea and offshore installations are inherently subject to a number of threats and, as part of a variety of legal, regulatory, and operational requirements, take steps to protect their personnel, assets, and operations. PMSCs may be engaged to assist in these efforts. PMSCs provide a range of essential services from assessing risk and providing advice on ship hardening, to the provision of armed guards aboard ships in high risk areas. The nature of the security services provided are intended to operate within the context of a protective measure and not a measure that is intended to project the will of the international community or state(s). This guidance *Standard* is applicable for any type of PMSC providing security services and operating at sea. The purpose of this guidance *Standard* is to improve and demonstrate the quality of services provided by PMSCs while maintaining the safety and security of their operations and clients (ship owner and/or charterer) within a framework that aims to ensure compliance with applicable and relevant international law (including human rights law), international maritime law, and law of the sea, flag and coastal state laws (civil and criminal), and commitments under the *International Code of Conduct* (ICoC) to respect human rights. This guidance draws on the International Maritime Organization (IMO) Circulars 1405, 1406, and 1443 which provide interim guidance regarding the use of private maritime security companies.

This *Standard* builds on the requirements found in the ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations - Requirements with Guidance* and/or the ISO 9001:2008, *Quality management systems – Requirements* or ISO 28000:2007, *Specification for security management systems for the supply chain* standards. This guidance *Standard* used in conjunction with either the ANSI/ASIS PSC.1-2012 and/or the ISO 9001:2008 or ISO 28000:2007 provides a means against which independent third-party auditors and certification bodies can assess whether a PMSC is fit to provide security services at sea and has a management system in place to prevent, inhibit, monitor, and mitigate incidents and patterns of behavior aboard ships at sea that might impact adversely on shipping operations or bring the industry into disrepute by breaches of applicable and relevant laws and commitments under the ICoC.

[1] This standard follows IMO procedure in using the acronym PMSC for Private Maritime Security Companies. This should not be confused with the same acronym PMSC that has been used by the UN for many years to describe Private Military and Security Companies and is used inter alia by the General Assembly, the Human Rights Council and a specialist Intergovernmental Working Group on Private Military and Security Companies. This standard does not apply to private military companies.

PMSCs have become important elements for supporting clients in the prevention and suppression of piracy and other threats. PMSCs are companies that provide security services on ships during transits and voyages and other critical times. PMSC operations face a certain amount of risk due to their need to address threats related to criminal acts against ships, those on board, and cargo during attempts to damage, board, or control the ship. Furthermore, PMSCs operate in a unique and complex operating environment which includes international laws and regulations, the movement between different coastal state jurisdictions, and the legal issues surrounding operations on the high seas. The challenge is to determine how to cost-effectively manage risk while meeting the organization's strategic and operational objectives within a framework that protects the safety and security of internal and external stakeholders including clients. PMSCs need to conduct their business and provide services in a manner that complies with international, national, coastal and flag state laws and local statutory and regulatory law, as well as the authority of the Master. PMSCs and their clients have an obligation to carry out due diligence to prevent incidents, mitigate and remedy the consequences of incidents, document and report them when they occur, and take corrective and preventive actions to avoid a reoccurrence.

Organizations seeking independent third-party certification can use the guidance in this *Standard* in conjunction with the requirements of either the ANSI/ASIS PSC.1-2012 and/or ISA9001:2008 or ISO 28000:2007, to demonstrate to clients, flag states, and national authorities that the PMSC is in conformance with the ANSI/ASIS PSC.1-2012 and/or ISA9001:2008 or ISO 28000:2007 standards. The guidance of this *Standard* is intended to be incorporated into any organization's management system based on the Plan-Do-Check-Act (PDCA) model; it is not intended to promote a uniform approach to all organizations. The design and implementation of quality assurance plans, procedures, and practices should take into account the particular requirements of each organization and their clients.

0.2 Respect for Human Rights and Legal Obligations

PMSCs assist clients by providing deterrence and protective measures for the protection of personnel as well as the ship and its operations in accordance with the contract. In addition to the role played by PMSCs, state forces are involved in the suppression of piracy and counter-piracy operations, including the detainment and prosecution of pirates. Armed response or use of firearms and other weapons as a response should be avoided in preference to protective and deterrence measures, including those described in current good management practices for ships, which are applicable wherever piracy and armed assault present a threat. Appropriate protective and defensive measures by onboard PMSCs is paramount, with less-than-lethal or non-lethal options used first, and the use of firearms and other weapons or armed response being used as a measure of last resort.

In providing protection, the PMSC is governed by various laws, regulations, and ethical norms associated with the use of force. PMSCs should take account of the relevant and applicable international, national, coastal and flag state laws and local statutory and regulatory law, in establishing their rules for the use of force, recognizing the individual's inherent right to self-defense. Because clients and their security teams have the obligation to comply with legal and

regulatory requirements, the provisions for rules for the use of force should be set out in the contract between the client and the PMSC, which should also specify the unambiguous rules to apply for a specific transit in terms of the laws of the flag and coastal states of the ship which are relevant to the ship's operations. The contract should specify that measures to assure the safety and security of the ship and those on board must be proportionate, that primary emphasis should be placed on deterrence and if force is necessary, there should be a graduated approach. Provisions in the contract should consider:

a) Compliance with applicable and relevant provisions of international law, international maritime law, and law of the sea;
b) Laws and regulations of national, coastal and flag states; and
c) International employment law and conventions.

The ANSI/ASIS PSC.1-2012 makes reference to the *Montreux Document* (2008) which encapsulates relevant rules of international law and good practices for PSC operations during armed conflicts The ICoC provides principles for PSCs to abide by in regions of weakened governance and disaster areas. Though the ICoC does not specifically address the maritime environment, the principles on which it rests, including respect for human rights, are applicable in the maritime environment. Therefore, clients and PMSCs have a shared responsibility to assure conformance with the principles on which the ICoC rests[2]. Therefore, in applying this *Standard*, key concepts should be considered as follows:

a) Respect for human rights;
b) Respect for relevant and applicable principles of international maritime law and law of the sea, as well as the relevant and applicable principles articulated in international humanitarian and human rights law;
c) Respect for the applicable and relevant international, national, coastal and flag state, and local statutory and regulatory laws associated with the ship, those on board the ship, its cargo and the legitimate and appropriate employment of persons;
d) Measures to assure the security and safety of the ship and those on board are proportional to the level of risk;
e) Non-violent and non-lethal measures should be applied first; and
f) When taking steps to deter or dissuade hostile action against the ship or those on board, such responses should use the minimum force necessary.

This standard, used in conjunction with the ANSI/ASIS PSC.1-2012, can help PMSCs to demonstrate to clients that they can provide services that are reliable, professional, and consistent with the ICoC. Furthermore, it provides a framework for PMSCs to define their operations within the maritime environment where legal requirements are complex.

[2] The Montreux document restates rules of international law and provides a set of good practices for States and their obligations to ensure that private military and security companies operating in circumstances of armed conflict comply with international humanitarian and human rights law. Though the Montreux document does not address the maritime environment, the good practices for contracting states, described in Part Two of the Montreux Document, should be considered as guidance by clients in their contracting practices with PMSCs.

0.3 Authorities, Obligations, and Responsibilities of Ship Master and Clients

The shipmaster (Master) has the ultimate responsibility for the security and safety of the ship, those on board, its cargo, and command of the ship. The decisions of the Master are expected to be guided by those that possess appropriate knowledge, skills, experience, and training. Therefore, the Master has the overall authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of PMSCs, clients, and/or naval forces as may be necessary. According to *Safety of Life at Sea (SOLAS)* the Master retains authority over the PMSC and its use of force, in accordance with the contract. Individuals within PMSC security teams retain their inherent right of self-defense.

The Master ensures that the ship complies with international, national, coastal and flag state, and local statutory and regulatory laws, in addition to company policies, and compliance with the ship's security plan as required by the ISPS Code. The Master is also ultimately responsible, under SOLAS, for aspects of operation such as the security and safe navigation of the ship, assuring seaworthiness of the ship, management of all personnel and crew, appropriate handling of all cargo, inventory of ship's cash and stores, and maintaining the ship's certificates and documentation.

The Master and designated Ship Security Officer (SSO), Company Security Officer (CSO), and/or Vessel Security Officer (VSO), in accordance with the International Ship and Port Facility (ISPS) Code are responsible for:

a) Implementation and maintenance of a Ship Security Plan;
b) Managing and monitoring ship’s security systems and processes; and
c) Training and motivating crew to perform security duties.

The client (owner or operator of the vessel) is responsible for informing the flag state, underwriters, charterers, and the protection and indemnity club that it will be engaging the services of PMSCs and whether they will be unarmed or armed. The Master serving as the client’s “agent of necessity” is directed (as part of the instructions of the client) as to whether or not PMSCs will be on board.

The client, or Master on his behalf, is responsible to:

a) Obtain the latest information regarding potential deliberate, accidental, or natural threats to the ship, those on board, its cargo, and its operations. This includes contacting reporting centers that are involved in activities associated with the protection of commercial shipping in the route of the transit (e.g., Maritime Security Centre Horn of Africa and NATO Shipping Center), as well as other relevant information sources;
b) Review the Ship Security Assessment and preparation and implementation of the Ship Security Plan as required by the ISPS Code;
c) Based on the current threat assessment, set the appropriate security level in accordance with the ship security plan, company guidelines, or at the direction of the relevant legal authority;

d) Prepare an Emergency Communication Plan including emergency contact numbers and prepared message;
e) Ensure the Ship Security Plan is in place for the passage through high risk areas at the designated security level;
f) Plan the route through the high risk areas, based on the risk assessment;
g) As applicable to the service being provided, to ensure that it has clearly delineated in the contract any parameters associated with the loading, embarking, issuance, control, use (including under the rules for the use of force), disembarkation, and – if necessary – emergency destruction of any weapons brought on board;
h) Provide a safe and secure location for the storage of firearms, other weapons, and ammunition, as well as relevant optics and ancillaries onboard the ship;
i) Verify the inventory of firearms and other weapons. Keep a copy in a safe place;
j) Conduct training and briefing of those on board and security operatives that reflects both the specific circumstances of the transit and the nature of the contract and respective roles, and attention to the obligations for respect for human rights;
k) Conduct debriefing sessions post transit;
l) Ensure that guidance and advice associated with good management practices (and other guidance as appropriate) is considered as a baseline requirement and incorporated to the extent possible without compromising the safety or security of those on board. This does not preclude the need for other security measures to be implemented where warranted by the risk assessment;
m) Ensure the size of the security team is consistent with the risk assessment and the total number of persons on board should not exceed the ship's safe manning certificate;
n) Establish an incident reporting mechanism consistent with legal requirements; and
o) Continuous oversight, monitoring, assessment, and improvement.

The Master has overall authority and responsibility for safety of the ship, its cargo, and those on board. This includes the authority and responsibility:

a) To authorize the use of force to protect those on board from the threat of crime or piracy;
b) For the safety, well-being, and legal treatment of any unauthorized persons including stowaways or pirates that have been apprehended;
c) For the safe navigation of the ship;
d) To abide by applicable and relevant international, national, coastal and flag state, and local statutory and regulatory laws including UNCLOS and SOLAS;
e) The apprehension and detention of persons pursuing criminal acts against the ship and its human and physical assets;
f) Incident reporting and preservation of evidence;
g) To determine whether the ship will respond to a distress signal; and
h) To follow good management practices for addressing the threat of crime and piracy, including ensuring the ship is sufficiently hardened, any citadel is fit for service and has ample supplies and HVAC controls, and that the ship appropriately communicates to relevant authorities regarding its presence in any high risk areas, as well as any threats perceived or delivered in that area.

Defined and documented procedures for the use of force, in accordance with international, national, coastal and flag state, and local statutory and regulatory laws, should be agreed in advance between the PMSC and the client, for specific transits. The Master cannot order PMSC personnel to open fire outside the agreed upon rules for the use of force or jurisdictional law. The Master's authority to order the PMSC to cease-fire does not negate the individual's right to self-defense in accordance with national and international laws. PMSC personnel have the right to use force, proportional to the threat presented, in order to prevent loss of life or serious injury to themselves or others.

0.4 PMSCs Obligations and Responsibilities

PMSCs also have specific obligations and responsibilities that should be considered when applying this standard. Obligation and responsibilities of PMSCs include:

a) Ensuring that the PMSC and persons working on its behalf abide by applicable and relevant international, national, coastal and flag state, and local statutory and regulatory laws at all times;
b) Ensuring the PMSC operates in accordance with the contract and persons working on its behalf on board the ship operate at all times under the authority of the Master;
c) Ensuring persons working on its behalf are adequately screened/vetted;
d) Ensuring persons working on its behalf are appropriately trained and equipped;
e) Advising the Master in a timely fashion regarding threats to the ship and recommending countermeasures, including:
    i. Preparing the ship, with the participation and contribution of the ship's crew, against threats and potential or actual disruptive incidents in accordance with the contract;
    ii. Agreeing and documenting in advance precise lines of authority and procedures in the event of a threat or disruptive incident;
    iii. Advising possible routing changes in the light of evolving intelligence reports and international liaison; and
    iv. Ensuring all incidents are appropriately documented and reported, particularly in the use of force or escalation of force.
f) The legal transport and handling of firearms and other weapons, including the maintenance of inventory documents and evidence of compliance with export control and counter proliferation regulations;
g) Ensuring all relevant licenses – including those for the security personnel and firearms and other weapons – are in place and are consistent with the law of the coastal and flag state;
h) Ensuring that their personnel respect and do not violate human rights;
i) Validating a threat, where practicable, before applying appropriate use of force;
j) Ensure that all of the rights and legal protections of security teams are respected; and
k) Abiding by good practices applicable to the industry.

The size and composition of the security team and equipment used by the PMSC should be determined in consultation with the shipowner. Considerations should include:

a) A security risk assessment for the ship's voyage, type of ship, threat environment of passage route, and necessary redundancies in the case of injury or illness;
b) Based on the risk assessment, and in consultation with the shipowner and Master, a decision regarding necessary protective measures for the voyage, including the need for armed security and equipment;
c) A clear hierarchy within the security team;
d) An appropriate skill and experience mix to address the tasks set out in the contract, including competence in risk assessments, protection measures, relevant languages, and medical aid;
e) Appropriate medical equipment and expertise to provide medical aid;
f) The appropriate type, carriage, and use of firearms and all other weapons to allow for a graduated level of deterrence when the decision is made to deploy armed security; and
g) Appropriate equipment, procedures, and training for the documentation and preservation of evidence in the event of an incident.

0.5 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 provides the framework for continual improvement to increase the likelihood of enhancing the quality of services while assuring the respect for human rights. It provides confidence to both the organization and its clients that the organization is able to manage its safety, security, and legal obligations.

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. This management systems standard provides guidance for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's management system for quality assurance of private security services.

The management system will enable PMSCs to analyze the requirements of clients and international obligations and define the processes that contribute to success. It also provides the framework for continual improvement in safety and security in order to enhance the quality of services the PMSC can deliver while meeting its legal obligations. The PMSCs which have adopted other management systems such as ANSI/ASIS SPC.1-2009, ANSI/ASIS PSC.1-2012, ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005, ISO 28000:2007, or OHSAS 18001:2007 can use their existing management system as a foundation for this security management system.

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

a) Understanding an organization's risk, security, safety, legal and human rights requirements;
b) Establishing a policy and objectives to manage risks;
c) Implementing and operating controls to manage an organization's risk and security requirements within the context of applicable and relevant international, national, coastal and flag state, and local statutory and regulatory laws, and the respect for human rights as articulated in the principles of the ICoC;
d) Monitoring and reviewing the performance and effectiveness of the Management System, administratively and operationally; and
e) Continual improvement based on objective measurement.

This *Standard* adopts the PDCA model, which is applied to structure the quality assurance processes. Figure 1 illustrates how a management system takes as input the quality assurance and security management requirements and expectations of the stakeholders, and through the necessary actions and processes produces quality assurance and risk management outcomes that meet those requirements and expectations. Figure 1 also illustrates the links in the processes presented in this *Standard*.

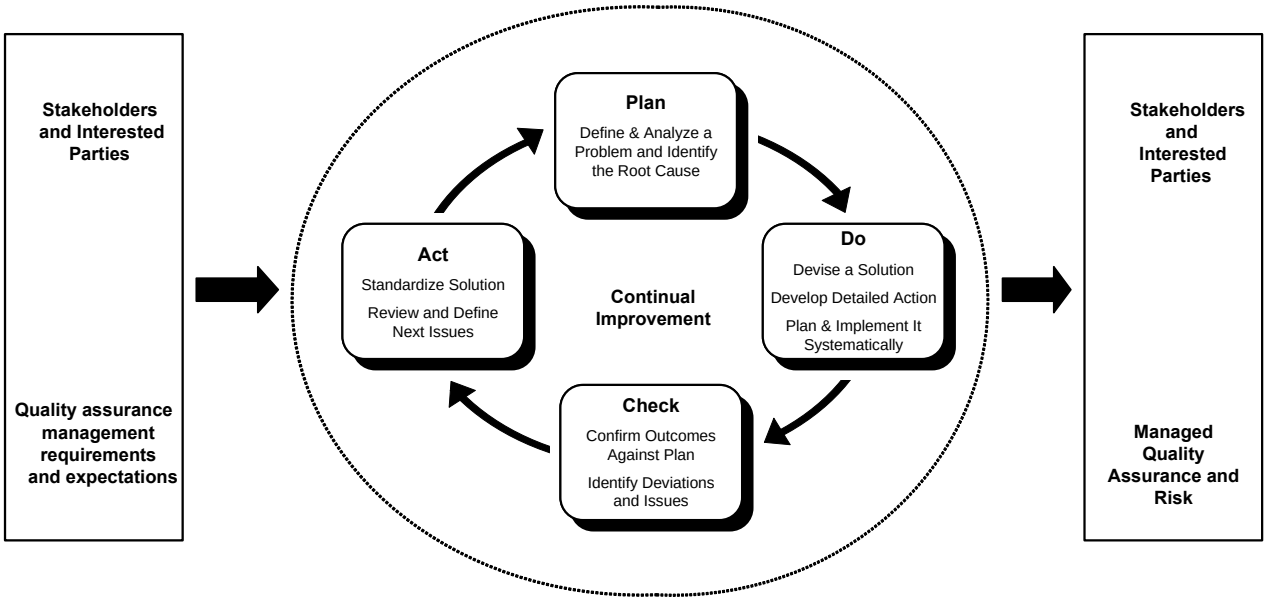

Figure 1: PDCA Model

PLAN (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing quality and improving risk management 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.

The PDCA model is a clear, systematic and documented approach to:

a) Set measurable objectives and targets;
b) Monitor, measure, and evaluate progress;
c) Identify, prevent, or mitigate problems as they occur;
d) Assess competence requirements and train persons working on the organization's behalf; and
e) Provide top management with a feedback loop to assess progress and make appropriate changes to the management system.

Furthermore, it contributes to information management within the organization, thereby improving operational efficiency.

Conformance with this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of ANSI/ASIS SPC.1-2009, ANSI/ASIS PSC.1-2012, ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005, ISO 28000:2007, OHSAS 18001:2007, and the PDCA Model.

Figure 2 illustrates the management systems approach used in ANSI/ASIS PSC.1-2012 and this *Standard*.

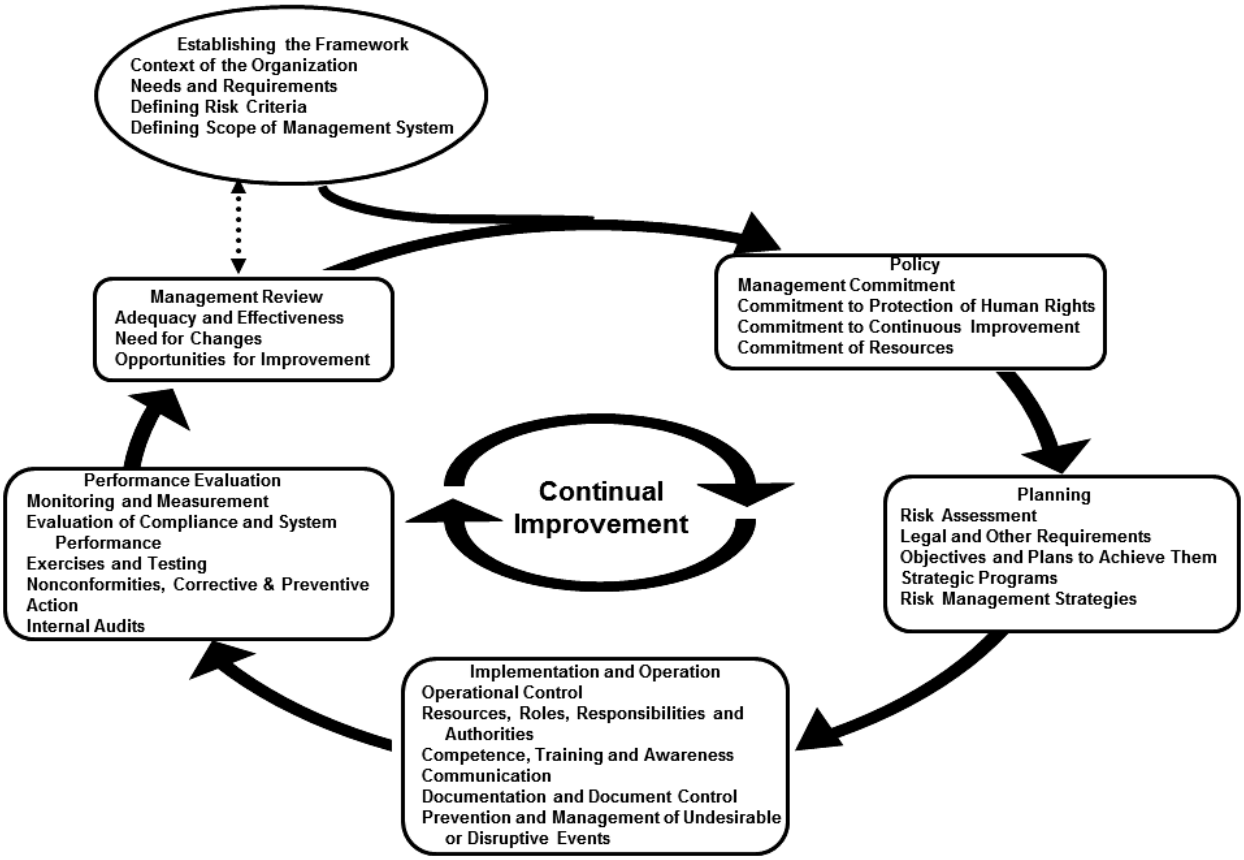

Figure 2: Quality Assurance and Security Management System (QASMS) Flow Diagram

Quality Assurance and Security Management for Private Security Companies Operating at Sea – Guidance

1. SCOPE

This *Standard* provides guidance for PMSCs to implement the ANSI/ASIS PSC.1-2012, *Management System for Quality of Private Security Company Operations – Requirements with Guidance* and/or the ISO 9001:2008, *Quality management systems – Requirements* or the ISO 28000:2007, *Specification for security management systems for the supply chain* standards. It provides the guidance for a Quality Assurance and Security Management System (QASMS) for Maritime Private Security Service Providers including Private Maritime Security Companies (collectively "PMSCs") to provide quality assurance in all security related activities and functions while demonstrating accountability to law and respect for human rights.

This *Standard* provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the management of their products and services. It is particularly applicable for any type of PMSC operating in a high risk environment at sea.

This *Standard* is applicable to any PMSC that needs to:

a) Establish, implement, maintain, and improve a QASMS;
b) Assess its conformity with its stated quality assurance and security management policy;
c) Demonstrate its ability to consistently provide services that meet client needs and are in conformance with applicable international, national, coastal and flag state, and local statutory and regulatory laws , as well as respect for human rights as articulated in the principles in the ICoC;
d) Provide a means whereby PMSC clients can conduct their own due diligence for the management of services retained from PMSCs;
e) Demonstrate conformity with the ANSI/ASIS PSC.1-2012 and/or ISO 9001:2008 or ISO 28000:2007 by:
    1) Making a self-determination and self-declaration;
    2) Seeking confirmation of its conformance by parties having an interest in the organization (such as clients);
    3) Seeking confirmation of its self-declaration by a party external to the organization; or
    4) Seeking certification/registration of its QASMS by an independent and accredited external organization[3].

[3] Organizations seeking third-party certification must do so with a certification body accredited to the ISO/IEC 17021:2011 *Conformity assessment – Requirements for bodies providing audit and certification of management systems* and the ANSI/ASIS PSC.2--2012, *Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations*.