Standard

Management System for Quality of Private Security Company Operations—Requirements with Guidance

Abstract

This Standard builds on the Montreux Document and the International Code of Conduct (ICoC) for Private Security Service Providers to provide requirements and guidance for a management system with auditable criteria for Quality of Private Security Company Operations.

The worldwide leader in security standards and guidelines development
MANAGEMENT SYSTEM FOR QUALITY OF PRIVATE SECURITY COMPANY OPERATIONS – REQUIREMENTS WITH GUIDANCE

A management systems approach for quality of private security services and the assurance of human rights

Approved March 5, 2012 (R2017)

American National Standards Institute, Inc.

ASIS International

Abstract

This Standard builds on the Montreux Document and the International Code of Conduct (ICoC) for Private Security Service Providers to provide requirements and guidance for a management system with auditable criteria for Quality of Private Security Company Operations, consistent with respect for human rights, legal obligations and good practices related to operations of private security service provider companies in conditions where governance and the rule of law have been undermined by conflict or disaster. It provides auditable requirements based on the Plan-Do-Check-Act model for third-party certification of private security service providers 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 shall not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

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

Copyright © 2017 ASIS International

ISBN: 978-1-934904-84-8
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.

This management systems standard provides generic auditable criteria and informative guidance.

About ASIS

ASIS International (ASIS) is the preeminent organization for security professionals, with 35,000 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.

About the Periodic Maintenance of the ANSI/ASIS PSC.1-2012

In 2017, ANSI/ASIS PSC.1-2012 underwent its five-year periodic maintenance and evaluation process under the Chairmanship of Dr. Rebecca DeWinter-Schmitt. The Technical Committee and Working Group agreed via consensus to reaffirm the standard with only minor, non-substantive changes. Thus, current users and implementers of ANSI/ASIS PSC.1-2012 will not find in this reaffirmed Standard any new, deleted or changed requirements. The minor changes ensure consistency in the language used to reference applicable national and international law, and consistency with the provisions of the two normative references, namely the Montreux Document and International Code of Conduct for Private Security Service Providers. Provisions on the necessary and reasonable use of force were clarified. Finally, the Bibliography was updated with useful references.

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 Group, Inc.
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
William J. Daly, Control Risks Security Consulting
Lisa DuBrock, Radian Compliance
Eugene F. Ferraro, CPP, PCI, CFE, Forensic Pathways, Inc.
Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc., Vice Chair
Robert W. Jones, Socrates Ltd
Glen Kitteringham, CPP, Kitteringham Security Group, Inc.
Michael E. Knoke, CPP, Retired, Chair
Bryan Leadbetter, CPP, Arconic
Jose M. Sobrón, United Nations
Roger D. Warwick, CPP, Pyramid Temi Group
Allison Wylde, Cardiff University

The Technical Committee and Working Group responsible for the review, had the following membership at the time it approved this document in 2017:

Committee Members

Committee Chair: Rebecca DeWinter-Schmitt, Ph.D., Human Analytics
Committee Secretariat: Aivelis Opicka, ASIS International

Christopher Aldous, CPP, PSP, Design Security
Lyle Alexander, CPP, A R M Specialists
Frank Amoyaw, LandMark Security
Deborah Avant, Josef Korbel School, University of Denver
Jose Barone Valdés, PSP, Barone Consulting Bureau
Mark Beaudry, CPP, IBM
Katherine Bell, CPP, Paladin Security
Dennis Blass, CPP, PSP, Children’s of Alabama
Michael Bouchard, CPP, Janus Global Operations
James Cameron, CPP, Security Concepts Group
John Casas, PSP, John Casas & Associates
Antony Chattin, MSS Global Ltd
Lawrence Clinton, Castor Vali Ltd
Georges Cowan, Business Continu-IT Partners
Oliver Cushing, Tsamota Certification Ltd
Jorge Dominguez, CPP, Lynx Technology Partners, Inc.
Jack Dowling, CPP, PSP, J D Security Consultants
Lisa DuBrock, Radian Compliance
Michael Edgerton, CPP, HudsonTrident
James Ellis, CPP, PSP, Principal Financial Group
Glynne Evans, Olive Group
Patricia Felt, Janus Global Operations
Mitchell Fenton, CPP, Baltusrol Golf Club
W Fitzgerald, CPP, Fitzgerald Technology Group
Mark Folmer, CPP, TrackTik
Nicholas Forster, FSI Worldwide Limited
Martina Gasser, Swiss Federal Department of Foreign Affairs
Joseph Gattuso, Sallyport Global Holdings
Sam Giles, United Kingdom Accreditation Service
Phillip Guffey, CPP, Roche Diagnostics Corp
Alison Hawkes, King’s College London
Robert Hulshouser, CPP, Urban Environmental Research, LLC
John Kemp, American K-9 Detection Services, LLC
Mitchell Kemp CHMM, CPP, Cummins Inc.
Glen Kitteringham, CPP, Kitteringham Security Group
Anaïs Laigle, ICoCA
Sorcha MacLeod, Free University Berlin and Berlin School of Law and Economics
Ronald Martin, CPP, Open Security Exchange
Christopher Mayer, U.S. Department of Defense
Oona Muirhead, MSS Global Ltd
Drew Neckar, CPP, ECMC Group
Ian Ralby, IR Consilium
James Schmitt, Human Analytics
Karel Simpson, GardaWorld International Protective Service
Jeffrey Slotnick, CPP, PSP, Setracon OR3M
Sally Smoczynski, Radian Compliance
Timothy Sutton, CPP, Compass Ventures, Inc.
Roger Warwick, CPP, Pyramid Temi Group
Sylvia White, GardaWorld International Protective Services
Michael White, CPP, Michael White Group
Andrew Williams, CPP, Pyramid Temi Group
Loftin Woodiel, CPP, Missouri Baptist University
Natalie Wykes, FSI Worldwide Limited
Andres Zaragoza, ICoCA
Working Group Members

Working Group Chair: Rebecca DeWinter-Schmitt, Ph.D., Human Analytics

Lyle Alexander, CPP, A R M Specialists
Frank Amoyaw, LandMark Security
Deborah Avant, Josef Korbel School, University of Denver
Jose Barone Valdés, PSP, Barone Consulting Bureau
Mark Beaudry, CPP, IBM
Katherine Bell, CPP, Paladin Security
Dennis Blass, CPP, PSP, Children’s of Alabama
James Cameron, CPP, Security Concepts Group
John Casas, PSP, John Casas & Associates
Antony Chattin, MSS Global Ltd
Jorge Dominguez, CPP, Lynx Technology Partners, Inc.
Lisa DuBrock, Radian Compliance
Michael Edgerton, CPP, HudsonTrident
James Ellis, CPP, PSP, Principal Financial Group
Glynne Evans, Olive Group
Mitchell Fenton, CPP, Baltusrol Golf Club
W Fitzgerald, CPP, Fitzgerald Technology Group
Mark Folmer, CPP, TrackTik
Nicholas Forster, FSI Worldwide Limited
Alison Hawks, King’s College London
Glen Kitteringham, CPP, Kitteringham Security Group
Anaïs Laigle, ICoCA
Sorcha MacLeod, Free University Berlin and Berlin School of Law and Economics
Christopher Mayer, U.S. Department of Defense
Oona Muirhead, MSS Global Ltd
Drew Neckar, CPP, ECMC Group
James Schmitt, Human Analytics
Karel Simpson, GardaWorld International Protective Service
Jeffrey Slotnick, CPP, PSP, Setracon OR3M
Sally Smoczynski, Radian Compliance
Sylvia White, GardaWorld International Protective Services
Michael White, CPP, Michael White Group
Natalie Wykes, FSI Worldwide Limited
Andres Zaragoza, ICoCA
Historical Information

At the time it approved this document in 2012, the PSC.1 Standards Committee, which is responsible for the development of this Standard, had the following members:

Committee Members

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

William Adkins, ESCOM
Christopher Aldous, CPP, PSP, Into Services Ltd
Lyle E. Alexander, CPP, A.R.M Specialists Ltd
Jacob Allen, Security Contracting Network
Thomas Allen, USAID
Frank P. Amoyaw, LandMark Security Limited
Raymond Andersson, Department of Defence - Australian Army
Edgard Ansola, CISA, CISSP, CEH, CCNA, ASEPEYO
Deborah Avant, University of California, Irvine
William Badertscher, CPP, Georgetown University
Pradeep Bajaj, Professional Industrial Security Management Academy
Colin Baldwin, Sustainability
Thomas Barnard, United States Attorneys' Office
Earl Basse, FCMA, CPP, CFE, Basse & Associates Inc.
Vladimir Batinic, CPO, G4S Secure Solutions (Canada) Ltd.
Andy Bearpark, British Association of Private Security Companies
Rene Beaulieu, CPP, SECuraGLOBE Solutions Inc.
Christopher Beese, Olive Group
Annyssa Bellal, Geneva Academy of International Humanitarian Law and Human Rights
Frank Bellomo, Business Risks International
Brian Bewley, MBA, Tactical Solutions International, Inc.
Donald Bitner, CPP, Amgen
Inge Black, CPP, CFE, CPO, CanAm Security Risk Group, LLC
Dennis Blass, CPP, PSP, CFE, CISSP, Children's of Alabama
Michael Bouchard, CPP, EOD Technology, Inc. (EODT)
Jeffrey Bozworth, O'Gara Training & Services LLC
Steve Brack, CPP, Noble Energy
Doug Brooks, ISOA
Anne-Marie Buzatu, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
James Cameron, Security Concepts Group
Jeffrey Campbell, CPP, U.S. Environmental Protection Agency
Chris Carter, RCDD, Affiliated Engineers Inc.
Paul Caruso, J.D., LL.M., AlliedBarton Security Services
John Casas, PSP, John Casas & Associates, L.L.C.
Andrew Clapham, Geneva Academy of International Humanitarian Law and Human Rights
Bruce W. Clark, TELUS Communications
Dick Clarke, Hart Security Ltd
Bob Cole, Minimal Risk Consultancy
Mark Conder, Independent Consultant
Ron Conlin, CPP, Eagles Eye Consultants
Peter Cook, Security Association for the Maritime Industry (SAMI)
Kevin Coon, Baker & McKenzie LLP-Global Law Firm
Hugues Costes, ArcelorMittal
Georges Cowan, Business Continu-IT Partners
Michael Crane, CPP, CFE, IPC International Corporation
Jonathan Crook, University of Essex
John Dalby, Marine Risk Management SA
Peter Davidsson, Cikralt AB
David Davis, CPP, Northrop Grumman
Renee de Nevers, Maxell School, Syracuse University
Rebecca DeWinter-Schmitt, Amnesty International USA
Mark DeWitt, J.D., Triple Canopy, Inc.
William Dill, Independent Consultant
J.C. Dodson, BAE Systems, Inc.
Mark Domanski, CPP, PSP, TaylorMade-adidas Golf Company
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
Lisa DuBrock, Radian Compliance
Eelco Dykstra, M.D., IKP Inc. (USA)
Nicholas Economou, MBA, Cablevision Systems Corporation
Michael Edgerton, CPP, Good Harbor Consulting, LLC
Hassan Ellaw, CISA, CISSP, SSCP, Cisco Systems
Heather Elms, Kogod School of Business, American University
Thomas Engells, CPP, The University of Texas Medical Branch at Galveston
David Feeney, AlliedBarton Security Services
Mitchell Fenton, CPP, MAS, BGC
Windom Fitzgerald, CPP, Pendulum Companies
Nicolas Florquin, Small Arms Survey
Mark Folmer, CPP, BECQ Group
Cory Forer, PSP, Abraxas Corporation
Jeremiah Frazier, CPP, CH2M HILL
Peter French, CPP, SSR Personnel
John Gargett, TRUSYS
Mark Gaudette, CPP, LPC, Big Y Foods, Inc.
Michael Goodboe, CPP, G4S Secure Solutions (USA), Inc.
Tahlia Gordon, Office of the Legal Services Commissioner
L. Earle Graham, CPP, G4S Secure Solutions (USA), Inc.
Chris Greyling, Pan African Security Association (PASA)
Kenneth J. Grossberger, CPP, Elite Investigations LTD
Stuart Groves, United Nations
Merlin Grue, PSP, Merlin Grue Investigative & Consulting Services
Phillip Guffey, CPP, Roche Diagnostics
Louis Gurvich, J.D., Gurvich Systems Inc./New Orleans Private Patrol
Sid Hamid, CPP, U.S. DHS/TSA OST
Suzanne Hart, Delaware Department of Transportation
Thomas Haueter, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Gary Hawkett, United Security Inc.
Alison Hawks, King’s College London
Louise Henderson, Aegis Defence Services Limited
Patrick Henderson, Protos Security
Krista Hendry, The Fund for Peace
Jerry Heying, CPP, International Protection Group, LLC
Lisa Hole, UK Ministry of Defence
J. B. Holeman, Oversight Inc.
Robert Hulshouser, CPP, Urban Environmental Research
Joshua Huminski, Aegis LLC
William Imbrie, DynCorp International, LLC
Fin Johnson, Ahtna Facility Services, Inc.
Brian Kaye, CBCP, Global Response Center, LLC
Mitchell Kemp, CPP, Cummins Inc.
Louis-Philippe Kernisan, CPP, Professional Security Services, S.A. /APAS
Graham Kerr, Hart Security Ltd.
Randy King, DOD Contractors.org, LLC
Christopher Kinsey, King’s College London
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Tony Koren, Blue Hackle North America LLC
Karl Kruse, University of California at Irvine
Kenneth Kurtz, Steele International
Misty Ladd, CPP, CPOI, Whelan Security
Mark LaLonde, Canpro Global
Billy Lamb, MBA, Stability Group Inc.
Todd Landman, Institute for Democracy and Conflict Resolution, University of Essex
Bill Lang, Independent Consultant
Steven Lente, CPP, Securitas Security Services USA, Inc.
Archie Lightfoot, G4S Risk Management Limited
Tim Lindsey, CPP, Paradigm Security Services, Inc.
Jeffrey J. Little, National Security Inspectorate
Thomas Loree, CPP, U.S. Army Corps of Engineers
Michael Love, CSC
Anthony Macisco, CPP, The Densus Group
Steve Mark, Office of the Legal Services Commissioner
Jonathan Marley, European Institute, London School of Economics
Christopher Mayer, U.S. Department of Defense
John McCaffery, Erinis International
Allan McDougall, PCIP, CMAS, CISSP, CPP, Evolutionary Security Management
Knut Erik Melstrom, Niscayah
Nils Melzer, Center for Business and Human Rights, University of Zürich
J. J. Messner, The Fund for Peace
Paul Mitchell, GlobalEdge International
Donald Moe, PPS, TCF Financial
J. Scott Mooneyham, U.S. Department of State, Diplomatic Security Service
Edgar Mosquera, Protection Resources International LLC
Jim Neidig, Independent Consultant
Loren Olson, PSP, JBA Consultants
Andrew Orsmond, Human Rights First
David Patterson, CPP, PSP, Steele International
Rodney Pettus, The Jones Group
Doug Petty, ITCLearn.com
Richard Phillips, Edinburgh International
Jason Pielemeier, U.S. Department of State, Bureau of Democracy, Human Rights and Labor
Mark Porterfield, CPP, CPOI, CHS III, Whelan Security
Werner Preining, CPP, CMAS, Interpool Security Ltd
William Prentice, Marine Security Initiatives, Inc.
Hugh Preston, 7 Bedford Row
Mitch Price, CPP, Florida State Security Services, Inc.
John Proctor, CGI
Daniel Puente Pérez, Sociedad de Prevención de Asepeyo
Mario Quijano, CPP, Electrolux
Erik Quist, EOD Technology, Inc. (EODT)
Ian Ralby, Ph.D., Security in Complex Environments Group, A|D|S Group, Ltd.
George Reed, Ph.D., University of San Diego
James Reese, TigerSwan Inc.
Devin Reynolds, CPP, Consultant
Kenneth Ribler, CPP, Senstar Inc.
Robert Riddell, CPP, The Cadillac Fairview Corporation Ltd.
Kristi Rogers, Aegis LLC
Eric Rojo, Magination Consulting International
Ronald Ronacher, PSP, CIPM, CMAS, Arup
Christopher Ruff, CPP, Santos
Vince Ruffolo, A&R Security
Chris Sanderson, Control Risks
Gavriel Schneider, CPP, MSEC, Dynamic Alternatives
Craig Schwab, CPP, AlliedBarton Security Services
Moshe Schwartz, Congressional Research Service
Timothy Shellenberger, CPP, Hershey Entertainment & Resorts
Matt Silcox, CPP, Independent Consultant
Gary Silverthorn, Secure Solutions & Design, LLC
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.
Nancy Slotnick, SPHR, GPHR, Setracon, Inc.
José Miguel Sobrón, United Nations
Eddie Sorrells, CPP, CHS IV, DSI Security Services
Teresa Stanford, CPP, Security Engineers, Inc.
Barry Stanford, CPP, AEG
Timothy Sutton, CPP, CHSS, Securitas Security Services USA, Inc.
Roger Sylvester, CPP, Ensign-Bickford Industries
Laurie Thomas, University of Findlay
Scott Thompson, Eagle Spirit Investigations LLC
Christine Tumolo, U.S. Security Care, Inc.
Michael Turner, ATP, CPS, Safe Passage Aviation Resources
Jonathan van Beek, Wilson Security
Karim Vellani, CPP, Threat Analysis Group, LLC
Erika Voss, CBCP, CORM, MBCI, Amazon
Roger Warwick, CPP, UNI
Scott Weber, CPP, Independent Consultant
Monte West, CPP, Blue Force, LLC
James E. Whitaker, CPP, PCI, CFE, UC Health
Allan Wick, CFE, CPP, PSP, Tri-State Generation & Transmission
Gavin Wilson, PSP, BHP Billiton
Guy Winter, Aegis Defence Services Limited
Loftin Woodiel, CPP, Ally Financial Services
Allison Wylde, CRM, MA, London Metropolitan University Business School

Working Group Members

Working Group Chairman: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
ANSI/ASIS PSC.1-2012 (R2017)

Lyle E. Alexander, CPP, A.R.M Specialists Ltd
Jacob Allen, Security Contracting Network
Raymond Andersson, Department of Defence - Australian Army
Frank Bellomo, Business Risks International
Brian Bewley, MBA, Tactical Solutions International, Inc.
Dennis Blass, CPP, PSP, CFE, CISSP, Children’s of Alabama
James Cameron, Security Concepts Group
John Casas, PSP, John Casas & Associates, L.L.C.
Rebecca DeWinter-Schmitt, Amnesty International USA
André du Plessis, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Johan du Plooy, CPP, Temi Group
Nicholas Economou, MBA, Cablevision Systems Corporation
Michael Edgerton, CPP, Good Harbor Consulting, LLC
Mitchell Fenton, CPP, MAS, BGC
Mark Folmer, CPP, BECQ Group
Tahlia Gordon, Office of the Legal Services Commissioner
Alison Hawks, King’s College London
Lisa Hole, UK Ministry of Defence
Robert Hulshouser, CPP, Urban Environmental Research
Brian Kaye, CBCP, Global Response Center, LLC
Billy Lamb, MBA, Stability Group Inc.
Tim Lindsey, CPP, Paradigm Security Services, Inc.
Steve Mark, Office of the Legal Services Commissioner
Christopher Mayer, U.S. Department of Defense
Allan McDougall, PCIP, CMAS, C|SSP, CPP, Evolutionary Security Management
Paul Mitchell, GlobalEdge International
J. Scott Mooneyham, U.S. Department of State, Diplomatic Security Service
Andrew Orsmond, Human Rights First
Doug Petty, JTCLearn.com
William Prentice, Marine Security Initiatives, Inc.
John Proctor, CGI
Erik Quist, EOD Technology, Inc. (EODT)
Ian Ralby, Ph.D., Security in Complex Environments Group, A|D|S Group, Ltd.
Devin Reynolds, CPP, Independent Consultant
Ronald Ronacher, PSP, CIPM, CMAS, Arup
Jeffrey Slotnick, CPP, PSP, Setracon, Inc.
Nancy Slotnick, SPHR, GPHR, Setracon, Inc.
Eddie Sorrells, CPP, CHS IV, DSI Security Services
Christine Tumolo, U.S. Security Care, Inc.
Allan Wick, CFE, CPP, PSP, Tri-State Generation & Transmission
# Table of Contents

1. **Scope** .......................................................................................................................... 1
2. **Normative References** ................................................................................................. 2
3. **Terms and Definitions** ................................................................................................. 2
4. **General Principles** ...................................................................................................... 2
   - 4.1 Leadership and Vision ............................................................................................ 3
   - 4.2 Governance ............................................................................................................ 3
   - 4.3 Need Oriented ........................................................................................................ 3
   - 4.4 Overall Organizational Risk Management Strategy .............................................. 4
   - 4.5 Systems Approach ................................................................................................ 4
   - 4.6 Adaptability and Flexibility .................................................................................. 4
   - 4.7 Managing Uncertainty ......................................................................................... 4
   - 4.8 Cultural Change and Communication ................................................................ 5
   - 4.9 Factual Basis for Decision Making ...................................................................... 5
   - 4.10 Continual Improvement ...................................................................................... 5
5. **Establishing the Framework** .................................................................................... 5
   - 5.1 General ................................................................................................................ 5
   - 5.2 Context of the Organization ................................................................................ 6
     - 5.2.1 Internal Context ............................................................................................ 6
     - 5.2.2 External Context .......................................................................................... 6
     - 5.2.3 Mapping and Analysis of Supply Chain and Subcontractors ...................... 7
   - 5.3 Needs and Requirements ....................................................................................... 7
   - 5.4 Defining Risk Criteria .......................................................................................... 7
   - 5.5 Scope of the Management System ...................................................................... 8
6. **Leadership** .................................................................................................................. 8
   - 6.1 General ................................................................................................................ 8
   - 6.2 Management Commitment .................................................................................... 9
   - 6.3 Statement of Conformance ................................................................................... 9
   - 6.4 Policy .................................................................................................................... 9
   - 6.5 Organizational Roles, Responsibilities, and Authorities ...................................... 10
7. **Planning** ..................................................................................................................... 10
   - 7.1 Legal and Other Requirements .......................................................................... 10
   - 7.2 Risk Assessment .................................................................................................. 11
     - 7.2.1 Internal and External Risk Communication and Consultation .............. 11
   - 7.3 Objectives and Plans to Achieve Them ................................................................ 12
   - 7.4 Action to Address Issues and Concerns .............................................................. 13
8. **Structural Requirements** ............................................................................................ 14
   - 8.1 Organizational Structure ....................................................................................... 14
   - 8.2 Insurance ............................................................................................................. 14
ANSI/ASIS PSC.1-2012 (R2017)

8.3 OUTSOURCING AND SUBCONTRACTING ................................................................................................................. 14
8.4 DOCUMENTED INFORMATION........................................................................................................................................ 14
  8.4.1 General.................................................................................................................................................................. 14
  8.4.2 Records.............................................................................................................................................................. 15
  8.4.3 Control of Documented Information.................................................................................................................. 15

9. OPERATION AND IMPLEMENTATION ....................................................................................................................... 16
  9.1 OPERATIONAL CONTROL........................................................................................................................................ 16
    9.1.1 General............................................................................................................................................................. 16
    9.1.2 Establishing Norms of Behavior and Codes of Ethical Conduct........................................................................ 16
  9.2 RESOURCES, ROLES, RESPONSIBILITY, AND AUTHORITY .................................................................................. 17
    9.2.1 Personnel.......................................................................................................................................................... 17
      9.2.1.1 Uniforms and Markings .............................................................................................................................. 17
    9.2.2 Selection, Background Screening, and Vetting of Personnel........................................................................... 17
    9.2.3 Selection, Background Screening, and Vetting of Subcontractors .................................................................... 18
    9.2.4 Financial and Administrative Procedures ....................................................................................................... 18
    9.2.5 Procurement and Management of Weapons, Hazardous Materials, and Munitions ................................. 19
  9.3 COMPETENCE, TRAINING, AND AWARENESS .................................................................................................. 19
  9.4 COMMUNICATION..................................................................................................................................................... 20
    9.4.1 Operational Communications.......................................................................................................................... 21
    9.4.2 Risk Communications........................................................................................................................................ 21
    9.4.3 Communicating Complaint and Grievance Procedures....................................................................................... 21
    9.4.4 Whistleblower Policy.......................................................................................................................................... 21
  9.5 PREVENTION AND MANAGEMENT OF UNDESIRABLE OR DISRUPTIVE EVENTS ............................................. 22
    9.5.1 Respect for Human Rights................................................................................................................................ 22
    9.5.2 Rules for Use of Force and Use of Force Training............................................................................................. 22
    9.5.3 Occupational Health and Safety........................................................................................................................ 22
    9.5.4 Performance of Security Functions..................................................................................................................... 23
    9.5.5 Incident Management........................................................................................................................................... 23
    9.5.6 Incident Monitoring, Reporting, and Investigations........................................................................................... 23
    9.5.7 Internal and External Complaint and Grievance Procedures .......................................................................... 24

10. PERFORMANCE EVALUATION ................................................................................................................................. 25
  10.1 MONITORING AND MEASUREMENT .................................................................................................................. 25
  10.2 EVALUATION OF COMPLIANCE........................................................................................................................ 25
  10.3 EXERCISES AND TESTING.................................................................................................................................... 25
  10.4 NONCONFORMITIES, CORRECTIVE AND PREVENTIVE ACTION ......................................................................... 26
  10.5 INTERNAL AUDIT .................................................................................................................................................. 26
  10.6 MANAGEMENT REVIEW ........................................................................................................................................ 27
    10.6.1 General............................................................................................................................................................. 27
    10.6.2 Review Input....................................................................................................................................................... 27
    10.6.3 Review Output.................................................................................................................................................... 27

11. IMPROVEMENT .......................................................................................................................................................... 28
  11.1 CHANGE MANAGEMENT......................................................................................................................................... 28
  11.2 OPPORTUNITIES FOR IMPROVEMENT ................................................................................................................ 28
  11.3 CONTINUAL IMPROVEMENT ................................................................................................................................ 28

A GUIDANCE ON THE USE OF THE STANDARD ........................................................................................................... 29
  A.1 INTRODUCTION ......................................................................................................................................................... 29
  A.2 HUMAN RIGHTS AND INTERNATIONAL LAW ...................................................................................................... 32
    A.2.1 Respect for Human Rights .................................................................................................................................. 32
    A.2.2 International Humanitarian Law .......................................................................................................................... 32
**A.10.3 Exercises and Testing** ..............................................................................................................................................69
A.10.4 Nonconformities, Corrective and Preventive Action ..................................................................................................................71
A.10.4.1 Corrective Action ............................................................................................................................................................71
A.10.4.2 Preventive Action ..............................................................................................................................................................72
A.10.5 Internal Audit .....................................................................................................................................................................72
A.10.6 Management Review ...........................................................................................................................................................73
A.11 Maturity Model for the Phased Implementation .......................................................................................................................74

**B TERMINOLOGY CONVENTIONS** ..............................................................................................................................................75

**C TERMS AND DEFINITIONS** ....................................................................................................................................................76

**D QUALIFIERS TO APPLICATION** ................................................................................................................................................85

**E BIBLIOGRAPHY** ........................................................................................................................................................................87

E.1 REFERENCES ............................................................................................................................................................................87
E.2 ASIS INTERNATIONAL PUBLICATIONS .....................................................................................................................................87
E.3 NATIONAL STANDARDS PUBLICATIONS3 .......................................................................................................................................87
E.4 ISO STANDARDS PUBLICATIONS4 ...........................................................................................................................................87
E.5 UNITED NATIONS AND INTERNATIONAL HUMAN RIGHTS PUBLICATIONS ...........................................................................88
E.6 OTHER REFERENCES ..................................................................................................................................................................89

---

**TABLE OF FIGURES**

**FIGURE 1:** PLAN-DO-CHECK-ACT MODEL ................................................................................................................................. XX
**FIGURE 2:** MANAGEMENT SYSTEM FOR QUALITY OF PRIVATE SECURITY COMPANY OPERATIONS FLOW DIAGRAM .................... XXII
**FIGURE 3:** PROCESS FOR MANAGING RISK ..............................................................................................................................43

---

**TABLE OF TABLES**

**TABLE 1:** VERBAL FORMS FOR THE EXPRESSION OF PROVISIONS ........................................................................................75
0. INTRODUCTION

0.1 General

Private Security Service Providers including Private Security Companies (collectively “PSCs”) play an important role in protecting state and non-state clients engaged in relief, recovery, and reconstruction efforts; commercial business operations; diplomacy; and military activity. This Standard is particularly applicable for any type of PSC operating in circumstances of weakened governances where the rule of law has been undermined due to human or naturally caused events. In unstable and dangerous environments where security and military operations are on-going, PSCs are engaged to provide enhanced security services in support of humanitarian, diplomatic, and military efforts, and to protect commercial activities including rebuilding of infrastructure. The PSC, in close coordination with legitimate clients and state actors, must adopt and implement the standards necessary to ensure that human rights and fundamental freedoms are adhered to in order to safeguard lives and property, and untoward, illegal, and excessive acts are prevented; while working under high risk conditions with the utilization of tactics, techniques, procedures, and equipment – including weapons. 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.

This Standard builds on the principles found in international human rights law and international humanitarian law (IHL). It provides auditable criteria and guidance that support the objectives of 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 of 17 September 2008 and the International Code of Conduct for Private Security Service Providers (ICoC) of 9 November 2010. This Standard provides a means for PSCs, and their clients, to implement the recommendations of the Montreux Document and to provide demonstrable commitment, conformance, and accountability to respect the principles outlined in the ICoC.

Given that PSCs have become important elements for supporting peace and stability efforts in regions where the capacity of societal institutions have become overwhelmed by human and natural caused disruptive events, their operations face a certain amount of risk. 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, security, and human rights of internal and external stakeholders, including clients and affected communities. PSCs need to conduct their business and provide services in a manner that respects human rights and laws. Therefore, they – and their clients – have an obligation to carry out due diligence to prevent incidents, mitigate, and remedy the consequences of incidents, report them when they occur, and take corrective and preventative actions to avoid a reoccurrence.

Protecting both tangible and intangible assets is a critical task for the viability, profitability, and sustainability of any type of organization (public, private, or not-for-profit). This transcends the
protection of just physical, human, and information assets but includes protecting the image and reputation of companies and their clients. Protecting assets requires a combination of strategic thinking, problem solving, process management, and the ability to implement programs and initiatives to correspond with the context of the organization’s operations and their risks.

Core to the success of implementing this Standard is embedding the values of the Montreux Document and ICoC into the culture and range of activities of the organization. Integrating these principles into management requires a long-term commitment to cultural change by top management, including leadership, time, attention, and resources – both monetary and physical. By using this Standard, organizations can demonstrate their commitment to integration of the principles of the Montreux Document and ICoC into their management system and their day-to-day operations. The Standard is designed to be integrated with other management systems within an organization (e.g., quality, safety, organizational resilience, environmental, information security, and risk standards). One suitably designed management system can thus fulfil the requirements of all these standards.

0.2 Human Rights Protection

While states and their entities must respect, uphold, and protect human rights, all segments of society (public, private, and non-governmental) have a shared responsibility to act in a way that respects and does not negatively impact upon human rights and fundamental freedoms (see Annex A.2).

Clients and PSCs have a shared responsibility to establish policies and controls to assure conformance with the principles of the Montreux Document and ICoC. By implementing this Standard, organizations can:

a) Establish and maintain a transparent governance and management framework in order to deter, detect, monitor, address, and prevent the occurrence and recurrence of incidents that have adverse impacts on human rights and fundamental freedoms;

b) Identify and operate in accordance with applicable international and national laws and regulations;

c) Conduct comprehensive internal and external risk assessments associated with safety, security, and human rights risks;

d) Implement risk control measures that support the rule of law, respect human rights of stakeholders, protect the interests of the organization and its clients, and provide quality services;

e) Ensure suitable and sufficient operational controls based on identified risks are implemented and managed to enhance the occupational health and safety, and welfare of persons working on behalf of the organization;

f) Effectively communicate and consult with public and private stakeholders;

g) Conduct effective screening and training of persons working on the organizations behalf;
ANSI/ASIS PSC.1-2012 (R2017)

h) Ensure that when the use of force is necessary, that such force is lawful and reasonable in intensity and duration;

i) Conduct performance evaluations of services rendered and the achievement of objectives; and

j) Develop and implement systems for reporting and investigating allegations of violations of applicable international and national law or human rights, as well as mitigating and remedying the consequences of undesired or disruptive events.

0.3 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 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, as well as respect human rights.

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 requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization’s management system for quality assurance of private security services. An organization needs to identify and manage many activities in order to function effectively. Any activity which enables the transformation of inputs into outputs, that uses resources and is formally managed, 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 for quality assurance management presented in this Standard encourages its users to emphasize the importance of:

a) Understanding an organization’s risk, security, and human rights protection requirements;

b) Establishing a policy and objectives to manage risks;

c) Implementing and operating controls to manage an organization’s risk and security requirements, and respect for human rights;

d) Monitoring and reviewing the performance and effectiveness of the Quality Assurance Management System (QAMS), administratively and operationally; and

e) Continual improvement based on objective measurement.
This Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the quality assurance processes. Figure 1 illustrates how a Quality Assurance Management System (QAMS) takes as input the quality assurance management requirements and expectations of the interested parties 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: Plan-Do-Check-Act 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:

- Set measurable objectives and targets;
- Monitor, measure, and evaluate progress;
- Identify, prevent or remedy problems as they occur;
- Assess competence requirements and train persons working on the organizations behalf; and
- 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.

This Standard is designed so that it can be integrated with quality, safety, environmental, information security, resilience, risk, security, and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards. Organizations that have adopted a management systems approach (e.g., according to ANSI/ASIS SPC.1-2009, ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005, ISO 28000:2007, OHSAS 18001:2007) may be able to use their existing management system as a foundation for the QAMS as prescribed in this Standard. Conformance with this Standard can be verified by an auditing process that is compatible and consistent with the methodology of ISO/IEC 17021:2011, Conformity assessment – Requirements for bodies providing audit and certification of management systems. Additional information on the conformance assessment process can be found in ANSI/ASIS PSC.2-2012, Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations.
Figure 2 illustrates the management systems approach used in this *Standard*.

Figure 2: Management System for Quality of Private Security Company Operations Flow Diagram
Management System for
Quality of Private Security Company Operations -
Requirements with Guidance

1. **Scope**

This *Standard* provides the principles and requirements for a Quality Assurance Management System (QAMS) for Private Security Service Providers including Private Security Companies (collectively “PSCs”) to provide quality assurance in all security related activities and functions while demonstrating accountability to law and respect for human rights. PSCs are organizations whose business activities include the provision of security services, either on its own behalf or on behalf of another. The *Standard* provides auditable criteria and guidance consistent with 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 of 17 September 2008* and the *International Code of Conduct for Private Security Service Providers (ICoC) of 9 November 2010*. This *Standard* provides a means for PSCs, and their clients, to provide demonstrable commitment and conformance with the aims of the *Montreux Document* and the principles outlined in the ICoC, as well as enhance the security and protection of stakeholders.

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 PSC operating in circumstances of weakened governances where the rule of law has been undermined due to human or naturally caused events.

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

- a) Establish, implement, maintain, and improve a QAMS;
- b) Assess its conformity with its stated quality assurance management policy;
- c) Demonstrate its ability to consistently provide services that meet client needs and are in conformance with applicable international and national laws, and human rights requirements;
- 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 clients);
  - III. Seeking confirmation of its self-declaration by a party external to the organization; or
  - IV. Seeking certification/registration of its QAMS by an independent and accredited external organization.