ASIS INTERNATIONAL

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

ANSI/ASIS PSC.1-2012

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL

Advancing Security Worldwide®

ANSI/ASIS PSC.1-2012

an American National Standard

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

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.

ISBN: 978-1-934904-33-6

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.

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

About ASIS

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

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

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

Commission Members

Charles A. Baley, Farmers Insurance Group, Inc.

Jason L. Brown, Thales Australia

Steven K. Bucklin, Glenbrook Companies, Inc.

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

Cynthia P. Conlon, CPP, Conlon Consulting Corporation

Michael A. Crane, CPP, IPC International Corporation

William J. Daly, Control Risks Security Consulting

Lisa DuBrock, Radian Compliance

Eugene F. Ferraro, CPP, PCI, CFE, Business Controls, Inc.

F. Mark Geraci, CPP, Purdue Pharma L.P., Chair

Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc.

Robert W. Jones, Socrates Ltd

Glen Kitteringham, CPP, Kitteringham Security Group, Inc.

Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair

Bryan Leadbetter, CPP, Bausch & Lomb

Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

Jose M. Sobrón, United Nations

Roger D. Warwick, CPP, Pyramid International

Allison Wylde, London Metropolitan University Business School

At the time it approved this document, the 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

Jerome Charles Conrad, U.S. Department of Homeland Security

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, Cikraitz 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

William Lutz Jr., NICET IV, Security On-Line Systems, Inc.

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, Erinys 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
Colin Walker, Mclean Walker Security Risk Management Inc.
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

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, CISSP, 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, ITCLearn.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

TABLE OF FIGURES

TABLE OF TABLES

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 preventive 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 local 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;

h) Ensure that the use of force is reasonably necessary, proportional, and lawful;
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 international law, local 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*.

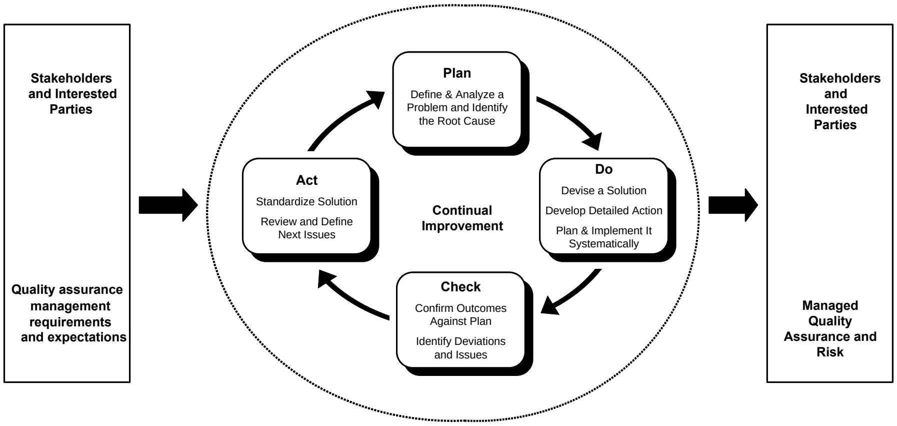
Stakeholders and Interested Parties
Quality assurance management requirements and expectations
Plan
Define & Analyze a Problem and Identify the Root Cause
Do
Devise a Solution
Develop Detailed Action
Plan & Implement It Systematically
Check
Confirm Outcomes Against Plan
Identify Deviations and Issues
Act
Standardize Solution
Review and Define Next Issues
Continual Improvement
Stakeholders and Interested Parties
Managed Quality Assurance and Risk

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:

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

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.2-201X[1], *Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations*.

[1] As of publication of this *Standard*, ANSI/ASIS PSC.2-201X is under review for approval.

Figure 2 illustrates the management systems approach used in this *Standard*.

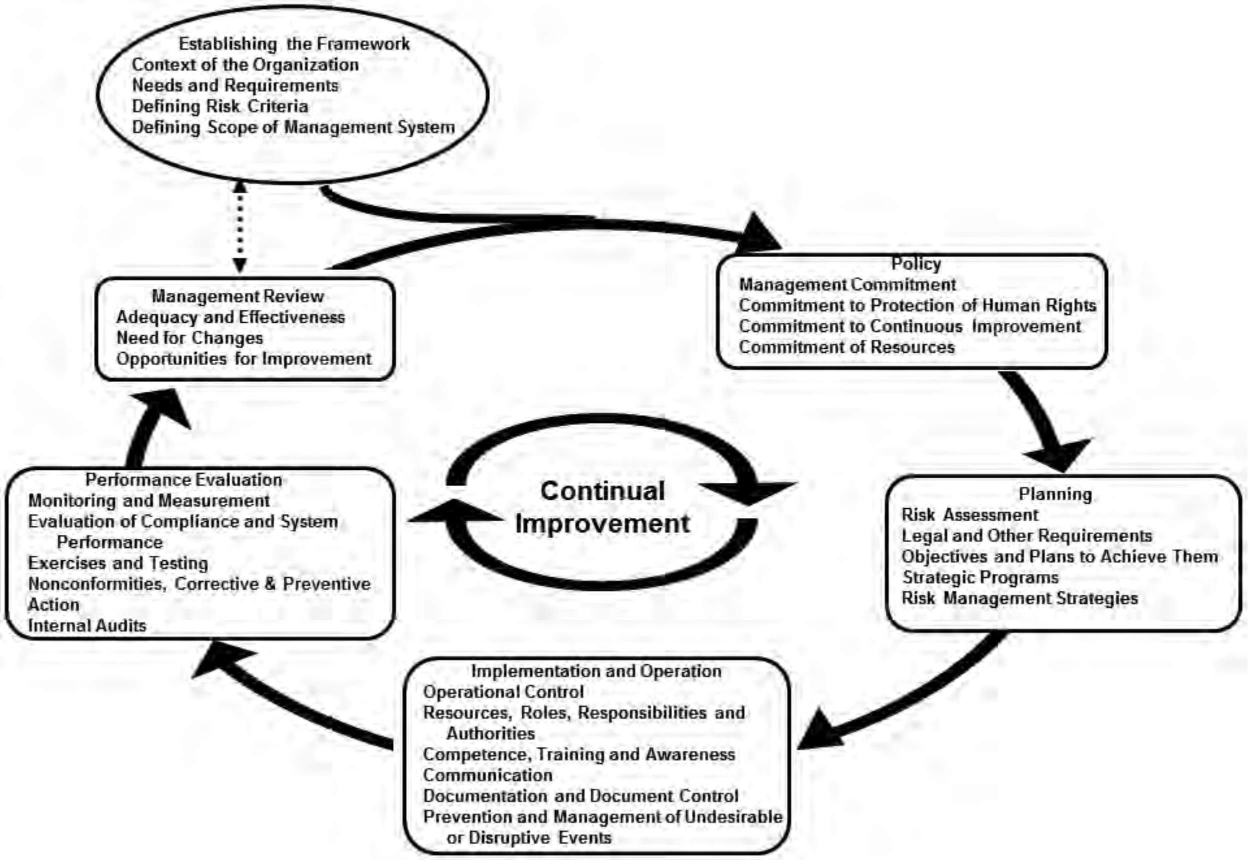
Establishing the Framework
Context of the Organization
Needs and Requirements
Defining Risk Criteria
Defining Scope of Management System
Policy
Management Commitment
Commitment to Protection of Human Rights
Commitment to Continuous Improvement
Commitment of Resources
Planning
Risk Assessment
Legal and Other Requirements
Objectives and Plans to Achieve Them
Strategic Programs
Risk Management Strategies
Implementation and Operation
Operational Control
Resources, Roles, Responsibilities and Authorities
Competence, Training and Awareness
Communication
Documentation and Document Control
Prevention and Management of Undesirable or Disruptive Events
Performance Evaluation
Monitoring and Measurement
Evaluation of Compliance and System Performance
Exercises and Testing
Nonconformities, Corrective & Preventive Action
Internal Audits
Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement
Continual Improvement

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 law, local 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.

The generic principles and requirements of this *Standard* are intended to be incorporated into any organization's management system based on the PDCA model; it is not intended to promote a uniform approach to all organizations in all sectors. The design and implementation of quality assurance plans, procedures, and practices should take into account the particular requirements of each organization: its objectives, context, culture, structure, resources, operations, processes, products, and services.

> NOTE: Consistent with the aims of the *Montreux Document*, PSC clients should use this Standard when retaining the services of PSCs. PSC clients should use the Standard's management system principles and requirements to conduct their own due diligence and management of services retained from PSCs. Clients should use this Standard to construct their contracting and contract administration process to support conformance with this Standard.

2. Normative References[2]

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

a) *Montreux Document On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict* (09/2008); and

b) *International Code of Conduct for Private Security Service Providers* (ICoC) (11/2010).

3. Terms and Definitions

An extensive Glossary of terms appears in Annex C.

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

4. General Principles

The goal of a QAMS is to support the provision of security services in circumstances of weakened governances where the rule of law has been undermined due to human or naturally caused events in a manner that enhances human safety and security as well as the protection of

[2] Please see Annex E, *Bibliography*, for where these documents are available.

assets (both tangible and intangible) while maintaining respect for international law, local laws, and human rights. PSCs need to conduct operations – and achieve clients' objectives – by managing risks to all stakeholders, including persons working on its behalf, affected communities, and their clients. This is accomplished by integrating legal, social, cultural, and environmental concerns into business operations and interactions with stakeholders when developing appropriate preemptive measures to protect the human and physical assets entrusted to their care. The intent is to minimize the likelihood and consequences of a disruptive or undesirable event (e.g., any event that has the potential to cause loss of life, harm to tangible or intangible assets, or negatively impact human rights and fundamental freedoms of internal or external stakeholders) by prevention, when possible; mitigating the impact of an event; through effectively and efficiently responding when an event occurs; by maintaining an agreed level of performance; by assuring accountability after the event; and by taking measures to prevent a recurrence. A QAMS will promote a culture in the organization that bonds quality of service with respect for international law, local laws, and human rights.

An acceptable quality of service is achieved by developing, designing, documenting, deploying and evaluating fit-for-purpose quality assurance systems. The elements for quality of security services are detailed in clauses 5-11 and the annexes of this *Standard*. In developing, applying and improving a quality of security service system, top management/decision-makers should apply the following general principles.

4.1 Leadership and Vision

Top management (which refers to the person or persons responsible for decision making, that have authorization for the implementation of the decisions) establishes the vision, sets objectives, and provides direction for the organization. They promote a culture of ownership within the organization where everyone views managing the risks of disruptive and undesirable events as part of their contribution to achieving the organization's goals and objectives. Top management demonstrates a commitment to promote a culture of quality of service coupled with a respect of international law, local laws, and human rights, and effective leadership in the implementation and maintenance of this *Standard*.

4.2 Governance

The assurance of the quality of services is viewed as part of an overall good governance strategy and an enterprise-wide responsibility. Quality of services in line with respecting international law, local laws, and protection of human rights is part of the organization's ethos and values. The protection of human life and safety in the course of achieving the mission's objectives is the primary concern of managing the risks of disruptive and undesirable events.

4.3 Needs Oriented

Assessing and understanding the organization’s assets, needs, and expectations is critical to the success and quality of private security operations management. Quality assurance management must be responsive to the needs and expectations of the client while also considering the needs and expectations of other stakeholders – such as affected communities, whose active or passive support is necessary for the success of the PSC and its client. Objectives of the organization are linked to internal and external stakeholder needs and expectations. Stakeholder relationships are systematically managed using a balanced approach between the needs of the organization, clients, and other stakeholders (such as affected communities).

4.4 Overall Organizational Risk Management Strategy

Quality assurance is part of an organization’s overall risk management strategy. Unless risk is managed effectively, organizations cannot maximize opportunities and minimize risk. Risk is the effect of uncertainty on the achievement of objectives, emphasizing human safety and security and the protection of assets (both tangible and intangible), while maintaining respect for international law, local laws, and human rights. The risk management process requires a clear understanding of the organization’s internal and external contexts to proactively identify opportunities and minimize risk. Assessing and understanding an organization’s acceptable level of risk is critical for the organization to develop a preemptive and effective risk management strategy that matches the needs and expectations of its internal and external stakeholders within the context of the operating environment's level of risk.

4.5 Systems Approach

A QAMS requires a multi-dimensional, iterative approach. Identifying, understanding, and managing interrelated processes and elements contribute to the organization's effective and efficient control of its risks. The systems approach examines the linkages and interactions between the elements that compose the entirety of the system. Component parts of a system can best be understood in the context of their interrelationships, rather than in isolation, and must be treated as a whole.

4.6 Adaptability and Flexibility

Most organizations, especially PSCs, operate in situations where the internal and external environments are subject to change. Organizations need to conduct on-going operational monitoring to identify changes and implement effective change control strategies. Organizations need to be adaptable: able and willing to evolve – constantly adapting to reflect the changing operating environment. The QAMS should be seen as a management framework, rather than a set of activities. As missions, budgets, priorities, and staff continue to change, the structure of the framework will remain predictable when particular applications change.

4.7 Managing Uncertainty

Quality assurance management is not always based on predictable threats and quantifiable risks. PSCs often work in high risk environments. Estimates and assumptions need to be made in analyzing the likelihood and consequences of threats, both known and unknown, and the vulnerability of the organization and interested parties within a changing environment. The management of risks of disruptive and undesirable events explicitly takes account of uncertainty, the nature of that uncertainty, and how it should be addressed.

4.8 Cultural Change and Communication

It is essential for top management to establish a well-defined strategy, communications, training, and awareness programs to ensure all levels of management and employees understand the goals of the management system. The QAMS supports cultural and perceptual change in the organization, thereby protecting the image and reputation of the organization and its clients. The QAMS must be fully understood and supported at the top level in the enterprise and communicated to all persons who work on behalf of the organization as part of the core culture of the organization.

4.9 Factual Basis for Decision Making

Assessing risk and managing quality of services drives decision making, and dictates the actions that will be taken based on factual analysis – balanced with experience and accepted industry best practices. The QAMS increases the ability to review, challenge, and change opinions and decisions; enhances problem-solving capacity; increases the ability to demonstrate effectiveness of past decisions through reference to factual records; and ensures that data and information are accurate, reliable, and timely – in line with company policy.

4.10 Continual Improvement

Managers improve their QAMS through the monitoring, measurement, review, and subsequent modification of QAMS processes, procedures, capabilities, and information within a continual improvement cycle. Formal, documented reviews are conducted regularly. The findings of such reviews should be considered by top management, and action taken where necessary to identify opportunities for improvement.

5. Establishing the Framework

5.1 General

The organization shall establish, document, implement, maintain, and continually improve a QAMS in accordance with the requirements of this *Standard*, and determine how it will fulfil these requirements. The organization shall continually improve its effectiveness in accordance with the requirements set out in this *Standard*. The QAMS shall incorporate and adopt the legal obligations and recommended practices of the *Montreux Document* relevant to PSCs and the guiding principles of the ICoC.

Where the organization chooses to subcontract or outsource any process or an activity that affects the conformity with the requirements of this *Standard*, the organization shall ensure and accept control and accountability over the operations of subcontractors in the performance of such processes. Control of such subcontracted or outsourced process or activity shall be identified and managed within the QAMS. Subcontractors of outsourced processes or services are also responsible and accountable for all client, legal, regulatory, ethical, and industry obligations.

5.2 Context of the Organization

The design and implementation of a management system framework is based on an understanding of the organization and its internal and external context of operation. Therefore, the organization shall define and document its internal and external context, including its supply chain and subcontractors. These factors shall be taken into account when establishing, implementing, and maintaining the organization's QAMS, and assigning priorities.

The organization shall evaluate internal and external factors that can influence the way in which the organization will manage risk.

5.2.1 Internal Context

The organization shall identify, evaluate, and document its internal context, including:

a) Strategies, policies, objectives, plans, and guidelines to achieve objectives;
b) Governance, roles and responsibilities, and accountabilities;
c) Values, ethos, and culture;
d) Information flow and decision-making processes;
e) Capabilities, resources, and assets;
f) Procedures and practices;
g) Activities, functions, services, and products; and
h) Brand and reputation.

5.2.2 External Context

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

a) The cultural and political context;
b) Legal, regulatory, technological, economic, natural, and competitive environment;
c) Contractual agreements, including other organizations within the contract scope;
d) Infrastructure dependencies and operational interdependencies;
e) Supply chain and contractor relationships and commitments;
f) Key issues and trends that may impact on the processes and/or objectives of the organization;
g) Perceptions, values, needs, and interests of external stakeholders (including local communities in areas of operation); and
h) Operational forces and lines of authority.

In establishing its external context, the organization shall ensure that the objectives and concerns of external stakeholders are considered when developing quality assurance management criteria.

5.2.3 Supply Chain and Subcontractor Node Analysis

Managing risks in the supply chain, including subcontractors, requires an understanding of the organization's culture and environment as well as the context of the global environment of its supply chain. Each node of the organization's supply chain involves a set of risks and management processes.

The organization shall identify and document its upstream and downstream supply chain, particularly its use of subcontractors, to identify significant risks and the potential to cause an undesirable or disruptive event. Managing supply chain risk shall be included in an organization's overall quality assurance management program where significant risks have been identified and there is a potential to cause an undesirable or disruptive event. The organization shall define and document the level in their supply chain and subcontractors to include in their quality assurance management program.

5.3 Needs and Requirements

Top management shall ensure that client requirements are identified, evaluated, and met to achieve the objectives of its contracts and minimize risks.

When identifying client needs and requirements, the organization shall determine:

a) Requirements specified by the client;
b) Statutory, regulatory, and human rights requirements applicable to the services;

c) Needs of the local and impacted communities and other stakeholders,
d) Impact and interactions of other PSCs and client operations;
e) Records and documentation requirements for delivery of services and non-conformances; and
f) Risk management requirements.

5.4 Defining Risk Criteria

The organization shall define and document criteria to evaluate the significance of risk. The risk criteria shall reflect the organization's values, objectives and resources. When defining the risk criteria the organization shall consider:

a) Critical activities, functions, services, products, and stakeholder relationships;
b) The operating environment and inherent uncertainty in operating in regions of weakened governance and rule of law;
c) The potential impact related to a disruptive or undesirable event;
d) Legal and regulatory requirements and other requirements (e.g., contractual obligations, human rights commitments) to which the organization subscribes;
e) The organization's overall risk management policy;
f) The nature and types of threats and consequences that can occur to its assets, business, and operations;
g) How the likelihood, consequences, and level of risk will be determined;
h) Needs of and impacts on stakeholders – particularly life, safety, and human rights;
i) Reputational and perceived risk;
j) Level of risk tolerance or risk aversion of the organization and its clients; and
k) How combinations and sequence of multiple risks will be taken into account.

5.5 Scope of the Management System

The organization shall define and document the scope of its QAMS, including the boundaries of the organization to be included in the QAMS – i.e., the whole organization, or one or more of its constituent parts. The organization shall define the scope of the QAMS in terms of and appropriate to its size, nature, and complexity from a perspective of continual improvement.

In defining the scope, the organization shall consider:

a) The organization's objectives, activities, internal and external obligations (including those related to stakeholders), and legal responsibilities; and

b) The uncertainty in achieving its objectives, including factors that could adversely affect the operations and activities of the organization within the context of their potential likelihood and consequences.

The organization shall define the scope consistent with the need to respect international law, local laws, and human rights while protecting and preserving the integrity of the organization – including relationships with stakeholders, interactions with key subcontractors, suppliers, outsourcing partners, and other stakeholders (for example, the organization's supply chain partners and suppliers, persons working on its behalf, clients, the community in which it operates, etc.).

Where an organization chooses to subcontract or outsource any process that affects conformity with the requirements of this *Standard*, the organization shall ensure that such processes are controlled. The controls and responsibilities of such outsourced processes shall be identified within the scope of the QAMS.

6. Leadership

6.1 General

Top management shall provide evidence of active leadership for the QAMS by overseeing its establishment and implementation, and motivating individuals to integrate quality assurance as a central part of the mission of the organization and its culture.

6.2 Management Commitment

Top management shall provide evidence of its mandate and commitment to the development and implementation of the QAMS and continually improving its effectiveness by:

a) Establishing the quality assurance policy;

b) Communicating to the organization the importance of meeting quality assurance management objectives and conforming to the QAMS policy, its legal responsibilities, and the need for continual improvement;

c) Providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the QAMS. Resources include people with specialized skills, equipment, internal infrastructure, technology, information, and financial resources; and

d) Conducting, at planned intervals, management reviews of the QAMS.

6.3 Statement of Conformance

Top management shall establish a Statement of Conformance with the principles of the:

a) *International Code of Conduct for Private Security Service Providers;*

b) *Montreux Document On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict*; and

c) Applicable IHL, human rights, and customary laws and agreements (see Annex A.2).

The Statement of Conformance shall be:

a) Documented, implemented, and maintained;

b) Communicated to and confirmed by all appropriate people working for or on behalf of the organization (including subcontractors);

c) Available to stakeholders; and

d) Visibly endorsed by top management.

6.4 Policy

Top management shall establish a quality assurance policy. The policy shall:

a) Provide a commitment to avoid, prevent, and reduce the likelihood and consequences of disruptive or undesirable events;

b) Be consistent with the organization's other policies;

c) Provide a framework for setting and reviewing quality assurance management objectives, targets, and programs;

d) Provide a commitment to comply with applicable legal and other requirements to which the organization subscribes;

e) Include a commitment to human rights and public safety as the first priority;

f) Be documented, implemented, and maintained;

g) Be communicated to all appropriate people working for or on behalf of the organization;

h) Be available to stakeholders;

i) Be visibly endorsed by top management;

j) Include a commitment to continual improvement; and

k) Be reviewed at planned intervals and when significant changes occur.

6.5 Organizational Roles, Responsibilities, and Authorities

Top management shall ensure that the responsibilities and authorities for relevant QAMS roles are assigned and communicated within the organization.

The organization shall appoint one or more individuals within the organization who – irrespective of other responsibilities – shall have defined competencies, roles, responsibilities, and authority for:

a) Ensuring that a QAMS is established, communicated, implemented, and maintained in accordance with the requirements of this *Standard*;
b) Identifying and monitoring the needs and expectations of the organization's internal and external stakeholders, and take appropriate action to manage these needs and expectations;
c) Ensuring that adequate resources are made available;
d) Promoting awareness of QAMS requirements throughout the organization; and
e) Reporting on the performance of the QAMS to top managers for review and as a basis for continuous improvement.

Top management shall ensure those responsible for the QAMS have the authority and competence to be accountable for the implementation and maintenance of the management system.

7. PLANNING

7.1 Legal and Other Requirements

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

a) Identify legal, regulatory, and other requirements to which the organization subscribes related to its personnel, facilities, activities, functions, products, services, supply chain, subcontractors, the environment, and stakeholders;
b) Identify relevant international humanitarian, human rights, and customary law and agreements (see annex A.2, Human Rights and International Law); and
c) Determine how these requirements apply to its operations.

The organization shall document this information and keep it up to date. It shall communicate relevant information on legal and other requirements to persons working on its behalf and other relevant third parties, including subcontractors. Private sector security organizations and their customers have a legal and ethical responsibility to comply with these obligations.

Any legal and regulatory requirements applicable to the organization's activities shall be identified and incorporated into the management of the organization's activities. Statutory requirements will vary between countries and jurisdictions. PSCs, as well as their clients, have an overriding obligation to minimize risk to human and public safety, and abide by international norms of human rights. The organization shall ensure that applicable legal, regulatory, and other requirements to which the organization subscribes are considered in developing, implementing, and maintaining its QAMS.

7.2 Risk Assessment

The organization shall establish, implement, and maintain a formal and documented risk assessment process for risk identification, analysis, and evaluation, in order to:

a) Identify tactical and operational risks due to intentional, unintentional, and natural threats that have a potential for direct or indirect consequences on the organization's activities, assets, operations, functions, and stakeholders, as well as its ability to abide by principles of human rights (threat, vulnerability, and criticality analysis);
b) Systematically analyze risk (likelihood and consequence analysis);
c) Determine those risks that have a significant impact on activities, functions, services, products, supply chain, subcontractors, stakeholder relationships, local populations, and the environment (significant risks and impacts); and
d) Systematically evaluate and prioritize risk controls and treatments and their related costs.

The organization shall:

a) Document and keep this information up to date and secure;
b) Periodically review whether the quality assurance management scope, policy, and risk assessment are still appropriate given the organization's internal and external context;
c) Re-evaluate risks within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships, and supply chains;
d) Evaluate the direct and indirect benefits and costs of options to manage risk and enhance reliability and resilience;
e) Evaluate the actual effectiveness of risk treatment options post-incident and after exercises;
f) Ensure that the prioritized risks and impacts are taken into account in establishing, implementing, and operating its QAMS; and
g) Evaluate the effectiveness of risk controls and treatments.

The risk assessment shall identify activities, operations, and processes that need to be managed, outputs shall include:

a) A prioritized risk register identifying treatments to manage risk;
b) Justification for risk acceptance;
c) Identification of critical control points (CCP); and
d) Requirements for supplier and contractor controls.

7.2.1 Internal and External Risk Communication and Consultation

The organization shall establish, implement, and maintain a formal and documented communication and consultation process consistent with operational security with internal and external stakeholders in the risk assessment process to ensure that:

a) Operational objectives and interests of the client (including the persons, organizations, communities, and/or activities being protected) are understood;
b) Risks are adequately identified and communicated;
c) Interests of other internal and external stakeholders are understood;
d) Dependencies and linkages with subcontractors and within the supply chain are understood;
e) Quality assurance risk assessment process interfaces with other management disciplines; and
f) Risk assessment is being conducted within the appropriate internal and external context and parameters relevant to the organization and its contractors and supply chain.

7.3 Objectives and Plans to Achieve Them

The organization shall establish, implement, and maintain documented objectives and targets to manage risks in order to anticipate, avoid, prevent, deter, mitigate, respond to, and recover from disruptive or undesirable events. Documented objectives and targets shall establish internal and external expectations for the organization, its contractors, and supply chain that are critical to mission accomplishment, product and service delivery, and functional operations.

Objectives shall be derived from and consistent with the quality assurance management policy and risk assessment, including the commitments to:

a) Minimize risk by reducing likelihood and consequence;
b) Respecting international law, local laws, and humans rights;
c) Financial, operational, and business requirements (including contractor and supply chain commitments); and
d) Continual improvement.

When establishing and reviewing its objectives and targets, an organization shall consider its financial, operational, and business requirements; the legal, regulatory, and other requirements; its human rights impacts; its significant risks; its technological options; and the views of stakeholders and other interested parties.

Targets shall be measurable qualitatively and/or quantitatively. Targets shall be derived from and consistent with the quality assurance management objectives and shall be:

a) To an appropriate level of detail;

b) Commensurate to the risk assessment;

c) Specific, measurable, achievable, relevant, and time-based (where practicable);

d) Communicated to all appropriate employees and third parties including subcontractors and supply chain partners with the intent that these persons are made aware of their individual obligations; and

e) Reviewed periodically to ensure that they remain relevant and consistent with the quality assurance management objectives and amended accordingly.

7.4 Action to Address Issues and Concerns

The organization shall establish, implement, and maintain quality assurance programs for achieving its objectives and risk treatment goals. The programs shall be optimized and prioritized in order to control and treat risks associated with its operations, subcontractors, and supply chain. The organization shall establish, implement, and maintain a formal and documented risk treatment process, which considers:

a) Removing the risk source, where possible;

b) Removing or reducing the likelihood of harm;

c) Removing or reducing harmful consequences;

d) Sharing the risk with other parties, including risk insurance;

e) Accepting risk through informed decision; and

f) Avoiding activities that give rise to the risk.

Top management shall:

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

b) Evaluate its quality assurance programs to determine if these measures have introduced new risks; and

c) Periodically review the risk treatment to reflect changes to the external environment, including legal, regulatory, and other requirements, and changes to the organization's policy, facilities, information management system(s), activities, functions, products, services, and supply chain.

8. Structural Requirements

The organization shall be a legal entity, or a defined part of a legal entity, with transparent ownership such that it can be held legally accountable for all its activities.

8.1 Organizational Structure

A clearly defined management structure shall identify roles, responsibilities, authorities, and accountabilities for its operations and services. The organization shall:

a) Document its organizational structure, showing duties, responsibilities, and authorities of management; and

b) Define and document if the organization is a defined part of a legal entity and the relationship to other parts of the same legal entity.

8.2 Insurance

The organization shall demonstrate that it has sufficient insurance to cover risks and associated liabilities arising from its operations and activities consistent with its risk assessment. When outsourcing or subcontracting services, activities, functions, or operations, the organization shall ensure sufficient insurance coverage for the subcontracted activities.

8.3 Outsourcing and Subcontracting

The organization shall have a clearly defined process wherein it describes the conditions under which it outsources activities, functions, or operations. The organization shall take responsibility for all activities outsourced to another entity. The organization shall have a legally enforceable agreement covering outsourcing arrangements including:

a) Commitment by subcontractors to abide by the same obligations as held by the organization and as described in this *Standard*;

b) Confidentiality and conflict of interest agreements;

c) Clear definition of provision of services; and

d) Conformance to the applicable provisions of this *Standard*.

8.4 Documented Information

8.4.1 General

The QAMS documentation shall include:

a) The quality assurance policy, Statement of Conformance, objectives, and targets;

b) A description of the scope of the QAMS;

c) A description of the main elements of the QAMS and their interaction, and reference to related documents;

d) Documented information required for the effective implementation and operation of the QAMS; and

e) Documents, including records, required by this *Standard*.

8.4.2 Records

The organization shall establish and maintain records to demonstrate conformity to the requirements of its QAMS.

Records include, among others:

a) Records required by this *Standard*;

b) Personnel screening;

c) Training records;

d) Process monitoring records;

e) Inspection, maintenance, and calibration records;

f) Pertinent subcontractor and supplier records;

g) Incident reports;

h) Records of incident investigations and their disposition;

i) Audit results;

j) Management review results;

k) External communications decision;

l) Records of applicable legal requirements;

m) Records of significant risk and impacts;

n) Records of management systems meetings;

o) Security, quality assurance, and human rights performance information; and

p) Communications with stakeholders.

The organization shall establish, implement, and maintain procedures to protect the sensitivity, confidentiality, and integrity of records including access to, identification, storage, protection, retrieval, retention, and disposal of records. Records shall be retained for a minimum of seven years or as otherwise required or limited by law.

8.4.3 Control of Documented Information

Documents required by the QAMS and by this *Standard* shall be controlled. The organization shall establish, implement, and maintain procedures to:

a) Approve documents for adequacy prior to issue;

b) Protect sensitivity and confidentiality of information;
c) Review, update as necessary, and re-approve documents;
d) Record amendments to documents;
e) Make updated and approved documents readily available;
f) Ensure that documents remain legible and readily identifiable;
g) Ensure that documents of external origin are identified and their distribution controlled;
h) Prevent the unintended use of obsolete documents; and
i) Ensure the appropriate, lawful, and transparent destruction of obsolete documents.

Organizations shall ensure the integrity of documents by rendering them securely backed-up, accessible only to authorized personnel, and protected from unauthorized disclosure, modification, deletion, damage, deterioration, or loss.

9. OPERATION AND IMPLEMENTATION

9.1 Operational Control

9.1.1 General

The organization shall identify the activities that are associated with the identified significant risks and consistent with its quality assurance management policy, risk assessment, objectives, and targets, in order to ensure that they are carried out under specified conditions, which will enable it to:

a) Comply with legal and other regulatory requirements;
b) Accomplish the mission while protecting the client's reputation;
c) Abide by local and applicable international laws, including international humanitarian, human rights, and customary laws, as well as other obligations as described in this *Standard*;
d) Ensure the security, well-being, and rights of both persons working on its behalf and local communities;
e) Implement risk management controls to minimize the likelihood and consequences of a disruptive or undesirable event; and
f) Achieve its quality assurance objectives and targets.

The organization shall establish, implement, and maintain documented procedures to control situations where their absence could lead to deviation from the QAMS policy, objectives, and targets.

9.1.2 Establishing Norms of Behavior and Codes of Ethical Conduct

The organization shall establish, implement, and maintain a Code of Ethics for norms of behavior for all persons working on its behalf, including employees, subcontractors, and outsource partners. The Code of Ethics shall be documented and clearly communicate respect for the human rights and dignity of human beings. The Code of Ethics shall ensure that all persons working on its behalf understand their responsibilities to prevent and report any abuses of human rights.

The organization shall communicate and document its Code of Ethics to all persons working on its behalf, as well as clients.

9.2 Resources, Roles, Responsibility, and Authority

Top management shall make available resources essential to establish, implement, maintain, and improve the QAMS. Resources shall include information, management tools, and human resources (including people with specialist skills and knowledge), and financial support.

Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective quality assurance management, including control, coordination, and command responsibility with a defined line of succession.

To effectively deal with disruptive and undesirable events, the organization shall establish planning, security, incident management, response and/or recovery team(s) with defined roles, appropriate authority, adequate resources including effective and safe equipment, and rehearsed operational plans and procedures.

9.2.1 Personnel

The organization shall retain sufficient personnel with the appropriate competence to fulfill its contractual obligations. Personnel shall be provided with adequate pay and remuneration arrangements, including insurance, commensurate to their responsibilities. The organization shall protect the confidentiality of this information as appropriate and provide personnel with relevant documents in language that is readily comprehensible for all parties.

The organization shall maintain documented information on all personnel:

a) As required by legal and contractual obligations;

b) To maintain contact with individuals and their immediate families;

c) To assist in personnel recovery in event of an incident; and

d) Needed for family notification of injury or death.

9.2.1.1 Uniforms and Markings

Consistent with the security of their clients, other civilians, and the requirements of law, the organization shall use uniforms and markings to identify its personnel and means of transport as belonging to the PSC organization whenever they are carrying out activities in discharge of their contract. This identification should be visible at a distance and distinguishable from those used by military and police forces. The organization shall establish and document procedures for use of uniforms and markings, as well as procedures for determining and documenting when such identification would be inconsistent with the requirements of this clause.

9.2.2 Selection, Background Screening, and Vetting of Personnel

The organization shall establish, document, implement, and maintain procedures for background screening and vetting of all persons working on its behalf to ensure they are fit and proper for the tasks they will conduct. Wherever possible, the screening shall include:

a) Consistency with legal and contractual requirements;

b) Identity, minimum age and personal history verification;

c) Education and employment history review;

d) Military and security services records check;

e) Review of possible criminal records;

f) Review reports of human rights violations;

g) Evaluation for substance abuse;

h) Physical and mental evaluation for fitness with assigned activities; and

i) Evaluation for suitability to carry weapons as part of their duties.

Minimum age requirements may be set by local law, laws applicable in the organization's legal domicile, or may be required of or by the client. In no case, however, shall any person younger than eighteen years of age be employed in duties that require them to use a firearm or other weapon.

Screening shall include an attestation by personnel that nothing in their present or past conduct would contradict the organization's Code of Ethical Conduct, Statement of Conformance, or adherence to the clauses of this *Standard*.

Background screening involves the disclosure of highly sensitive information; therefore, the organization shall develop procedures to appropriately and strictly secure the confidentiality of information both internally and externally. Records shall be maintained consistent with relevant statutes of limitations.

Selection of qualified personnel shall be based on defined competencies including knowledge, skills, abilities, and attributes. Both the screening and selection measures shall be consistent with legal and contractual requirements, as well as the good practices described in the *Montreux Document* and the principles in the ICoC.

9.2.3 Selection, Background Screening, and Vetting of Subcontractors

When the organization subcontracts activities, functions, and operations on a temporary or continuing basis, this work shall be placed with a competent subcontractor. The organization is responsible for the subcontractor's work and is liable, as appropriate and within applicable law, for the conduct of these subcontractors. The organization shall:

a) Ensure appropriate written contractual agreements with the subcontractor;
b) Advise the client of the arrangement in writing, and when appropriate obtain approval of the client;
c) Maintain a register of all subcontractors it uses;
d) Communicate the responsibilities of this *Standard* to the subcontractor; and
e) Maintain a record of evidence of conformance with this *Standard* for work subcontracted.

9.2.4 Financial and Administrative Procedures

The organization shall develop financial and administrative procedures to support quality assurance management program before, during, and after a disruptive or undesirable event. Procedures shall be:

a) Established to ensure that fiscal decisions can be expedited; and
b) In accordance with established authority levels and accounting principles; and
c) Established in consultation and coordination with the client.

9.2.5 Procurement and Management of Weapons, Hazardous Materials, and Munitions

The organization shall establish documented procedures and records for procurement and management of weapons, hazardous materials, explosives, and munitions, based on local and international legal and regulatory requirements and mission objectives and risks identified, including:

a) Compliance with registrations, certifications, and permits;
b) Acquisition;
c) Secure storage;
d) Controls over their identification, issue, use, maintenance, return, and loss;
e) Records regarding to whom and when weapons are issued;
f) Identification and accounting of all ammunition and weapons; and
g) Proper disposal with verification.

Provision of weapons shall be for self-defense, or the defense of others, and appropriate to the task and operations in accordance with accepted weaponry used by law enforcement agencies and consistent with appropriate international and national law.

9.3 Competence, Training, and Awareness

The organization shall ensure that all persons performing tasks on its behalf, including employees, subcontractors, and outsource partners, who have the potential to prevent, cause, respond to, mitigate, or be affected by identified risks are competent (on the basis of appropriate education, training, and experience), and shall retain associated records.

The organization shall identify competencies and training needs associated with quality assurance management, particularly the performance of each individual's functions, consistent with respect for legal obligations and human rights. It shall provide training or take other action to meet these needs, and shall retain associated records.

The organization shall establish, implement, and maintain procedures to ensure all persons performing tasks on its behalf are aware of:

a) The parameters of performance of their functions;

b) The significant hazards, threats, risks, and potential impacts associated with their work;

c) Applicable local and international laws, including criminal, human rights, and international humanitarian laws; including but not limited to:

- Prohibition of torture or other cruel, inhuman, or degrading treatment;
- Prohibition and awareness of sexual exploitation and abuse or gender based violence;
- Recognition and prevention of human trafficking and slavery; and
- Measures against bribery, corruption, and similar crimes.

d) The procedures to reduce the likelihood and/or consequences of a disruptive or undesirable event, including procedures to respond to and report events;

e) The use of weapons and force that is reasonably necessary, proportional, and lawful;

f) Communications protocols and procedures;

g) The culture, such as customs and religion, of the environment in which they are operating;

h) Receiving and transmitting complaints from civilian populations to the appropriate authority;

i) The importance of conformity with the QAMS policy and procedures, and with the requirements of the QAMS;

j) Their roles and responsibilities in achieving conformity with the requirements of the QAMS; and

k) The potential consequences of departure from specified procedures.

The organization shall provide physical, mechanical, and live-fire training and evaluation for all personnel authorized to carry lethal, less lethal, or non-lethal weapons in the performance of their duties. A documented level of competence shall be demonstrated with the specific weapons authorized as specified by the organization, or to a higher level as required by law or contractual obligations.

The organization shall build, promote, and embed a quality assurance management culture within the organization that:

a) Ensures the quality assurance management culture and respect for human rights becomes part of the organization’s core values and governance;

b) Makes stakeholders aware of the quality assurance management policy and their role in any plans; and

c) The benefits of improved personal performance.

9.4 Communication

The organization shall establish, implement, and maintain procedures for:

a) Communicating with staff and employees;

b) Communicating with external stakeholders including its clients, subcontractors, supply chain partners, the host government, the local and emergency services authorities, members of the community in which it operates, and the media;

c) Receiving, documenting, and responding to communications from internal and external stakeholders;

d) Defining and assuring availability of the means of communication during atypical situations and disruptions; and

e) Regular testing of communications system for normal and abnormal conditions.

Communication procedures shall consider the sensitive nature of operational information and legal restrictions on information sharing.

9.4.1 Operational Communications

The organization shall develop standardized communication procedures to share information about the security team activity, location, operational and logistic status, relevant threat information, and incident reporting to company management, clients, other PSC teams and relevant civil or military authorities. This shall include procedures for requesting immediate assistance from military or civil authorities, other security teams, and emergency medical support.

The organization shall ensure that spoken and written communications can be received and understood by all levels and operators and that all levels can respond in a language or means that can be understood by appropriate, internal and external stakeholders.

Security teams shall be able to communicate security related information to the party they are protecting in a form the protected party understands.

9.4.2 Risk Communications

The organization shall decide, based on safeguarding life as the first priority and in consultation with stakeholders, whether to communicate externally about significant risks and impacts to stakeholders and document its decision. If the decision is to communicate, the organization shall establish and implement (a) method(s) for this external communication, alerts, and warnings (including with the media).

9.4.3 Communicating Complaint and Grievance Procedures

Complaint and grievance procedures shall be communicated to internal and external stakeholders. Procedures shall minimize obstacles to access caused by language, educational level, or fear of reprisal, as well as consider needs for confidentiality and privacy.

9.4.4 Whistleblower Policy

The organization shall communicate to people working on its behalf, who have reasonable belief that a nonconformance of this *Standard* has occurred, their right to anonymously report the nonconformance internally, as well as externally to appropriate authorities. The organization shall not take any adverse action against any individual for the act of making a report in good faith.

9.5 Prevention and Management of Undesirable or Disruptive Events

9.5.1 Respect for Human Rights

The organization shall establish, implement, and maintain procedures to treat all persons with dignity and with respect for their human rights and to report any nonconformance. The organization shall develop and communicate to all persons working on its behalf procedures for conduct consistent with the principles of the *Montreux Document* and ICoC; as well as any contractual, legal, and regulatory requirement applicable to the organization's activities.

9.5.2 Rules for Use of Force and Use of Force Training

The organization shall identify competencies and training needs associated with the use of force and weapon-specific training. It shall provide ongoing training for the use of force as well as training to meet these needs of personnel carrying weapons. The organization shall verify competence and retain associated records.

The organization shall establish, document, and maintain procedures for the *Rules for the Use of Force (RUF*) compatible with RUFs specified by the client or a competent legal authority. The organization's RUF shall be consistent with local and international law and be subject to legal review before implementation. RUF includes conditions for the use of deadly force and less lethal force, emphasizing that deadly force is justified only under conditions of necessity when there is a reasonable belief that a person or persons presents an imminent threat of death or serious bodily harm to the individual or others in the vicinity. Force is used only when lesser means cannot be reasonably employed, or have failed, and the risk of death or serious bodily harm to innocent persons is not increased by its use. Use of force training shall be based on application of the approved RUF.

Use of force training shall include:

a) Reasonable steps to avoid the use of force;
b) Use of force continuum to resolve threats with minimum necessary force;
c) Use of force complies with all national and international obligations in a manner consistent with applicable law;
d) Use of force is proportionate to the threat and appropriate to the situation; and
e) Use of force against persons only in self-defense or defense of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life.

The organization shall provide training to avoid, identify, and report non-conformances in the use of force including the use of weapons, as well as for the mitigation of consequences.

9.5.3 Occupational Health and Safety

The organization shall establish, implement, and maintain procedures to promote a safe and healthy working environment including reasonable precautions to protect people working on its behalf in high-risk or life threatening operations consistent with legal, regulatory, and contractual obligations. Procedures shall include:

a) Assessing occupational health and safety risks to people working on its behalf as well as the risks to external parties;
b) Hostile environment training;
c) Provision of personal protective equipment, appropriate weapons, and ammunition;
d) Medical and psychological health awareness training, care, and support; and
e) Guidelines to identify and address workplace violence, misconduct, alcohol and drug abuse, sexual harassment, and other improper behavior.

9.5.4 Performance of Security Functions

The organization shall establish, implement, and maintain procedures to support the performance of security related tasks, including:

a) Observation and reporting;

b) Apprehension and detention of persons;

c) Search;

d) Actions on contact/react to direct or indirect fire;

e) First Aid, casualty care, and evacuation;

f) Incident reporting and evidence preservation; and

g) Other task and context specific functions required under the terms of a specific requirement or otherwise required by client or competent authority.

9.5.5 Incident Management

The organization shall establish, implement, and maintain procedures to identify undesirable and disruptive events that can impact the organization, its activities, services, stakeholders, human rights, and the environment. The procedures shall document how the organization will proactively prevent, mitigate, and respond to events.

When establishing, implementing, and maintaining procedures to expeditiously prepare for, mitigate, and respond to a disruptive event, the organization shall consider each of the following actions:

a) Safeguard life and assure the safety of internal and external stakeholders;

b) Respect human rights and human dignity;

c) Prevent further escalation of the disruptive event;

d) Minimize disruption to operations;

e) Notification of appropriate authorities;

f) Protect image and reputation (of the organization and its client); and

g) Corrective and preventative actions.

9.5.6 Incident Monitoring, Reporting, and Investigations

The organization shall establish, implement, and maintain procedures for incident monitoring reporting, investigations, disciplinary arrangements, and remediation. Incidents involving use of force or weapons, any casualties, physical injuries, allegations of abuse, loss of sensitive information or equipment, substance abuse, or nonconformance with the principles of the *Montreux Document* and ICoC, as well as applicable laws and regulations, shall be reported and investigated with the following steps taken, including:

a) Documentation of the incident;

b) Notification of appropriate authorities;

c) Steps taken to investigate the incident;

d) Identification of the root causes;
e) Corrective and preventative actions taken; and
f) Any compensation and redress given to the affected parties.

The organization shall assure all persons working on its behalf are aware of their responsibilities and the mechanisms to monitor and report non-conformances and incidents.

Records of non-conformances and incidents shall be maintained and retained for a minimum of seven years or as specified by legal or regulation requirements.

9.5.7 Internal and External Complaint and Grievance Procedures

The organization shall establish procedures to document and address grievances received from internal and external stakeholders (including clients and other affected parties). The procedures shall be communicated to internal and external stakeholders to facilitate reporting by individuals of potential and actual nonconformances with this *Standard*, or violations of international law, local laws, or human rights. The organization shall investigate allegations expeditiously and impartially, with due consideration to confidentiality and restrictions imposed by local law. The organization shall establish and document procedures for:

a) Receiving and addressing complaints and grievances;
b) Establishing hierarchical steps for the resolution process;
c) The investigation of the grievances, including procedures to;
    1) Cooperate with official external investigation mechanisms;
    2) Prevent the intimidation of witnesses or inhibiting the gathering of evidence; and
    3) Protect individuals submitting a complaint or grievance in good faith from retaliation.
d) Identification of the root causes;
e) Corrective and preventative actions taken, including disciplinary action commeasurable with any infractions; and
f) Communications with appropriate authorities.

Grievances alleging criminal acts, violations of human rights, or imminent danger to individuals shall be dealt with immediately by the organization, and other authorities as appropriate.

10. PERFORMANCE EVALUATION

The organization shall evaluate quality assurance management plans, procedures, and capabilities through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors should be reflected immediately in the procedures.

The organization shall keep records of the results of the periodic evaluations.

10.1 Monitoring and Measurement

The organization shall establish, implement, and maintain performance metrics and procedures to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its performance (including partnerships, subcontracts, and supply chain relationships). The procedures shall include the documenting of information to monitor performance, applicable operational controls, and conformity with the organization's quality assurance management objectives and targets.

The organization shall evaluate and document the performance of the systems which protect its assets (human and physical), as well as its communications and information systems.

10.2 Evaluation of Compliance

Consistent with its commitment to compliance, the organization shall establish, implement, and maintain procedures for periodically evaluating compliance with applicable legal, regulatory, and human rights requirements. The organization shall evaluate compliance with other requirements to which it subscribes. The organization may wish to combine this evaluation with the evaluation of legal compliance referred to above or to establish separate procedures.

The organization shall keep records of the results of the periodic evaluations.

10.3 Exercises and Testing

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

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

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

10.4 Nonconformities, Corrective and Preventive Action

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

a) Identifying and correcting nonconformities and taking actions to mitigate their consequences;
b) Evaluating the need for actions to prevent nonconformities and implementing appropriate actions designed to avoid their occurrence;
c) Investigating nonconformities, determining their root causes, and taking actions in order to avoid their recurrence;
d) Recording the results of corrective and preventive actions taken; and
e) Reviewing the effectiveness of corrective and preventive actions taken.

The organization shall ensure that proposed changes are made to the QAMS documentation.

10.5 Internal Audit

The organization shall establish, implement, and maintain a quality assurance management audit program and ensure that internal audits of the QAMS are conducted at planned intervals.

Internal audits shall assess whether the QAMS:

a) Meets the requirements of this *Standard*;
b) Meets relevant legal, regulatory, human rights, and contractual obligations;
c) Has been properly implemented and maintained;
d) Performed as expected; and
e) Has been effective in achieving the organization's QAMS policy and objectives.

The organization shall:

a) Plan, establish, implement, and maintain an audit program(s), taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits;
b) Define the audit criteria, scope, frequency, methods, responsibilities, planning requirements, and reporting;
c) Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process (e.g., auditors should not audit their own work);
d) Ensure that the results of the audits are reported to the management responsible for the area being audited; and
e) Retain relevant documented information as evidence of the results.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

10.6 Management Review

10.6.1 General

Management shall review the organization's QAMS at documented planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the QAMS, including the QAMS policy and objectives. The results of the reviews shall be clearly documented and records shall be maintained.

10.6.2 Review Input

The input to a management review shall include:

a) Results of QAMS audits and reviews;

b) Feedback from interested parties;

c) Techniques, products, or procedures that could be used in the organization to improve the QAMS performance and effectiveness;

d) Status of preventive and corrective actions;

e) Results of exercises and testing;

f) Risks not adequately addressed in the previous risk assessment;

g) Incident reports;

h) Results from effectiveness measurements;

i) Follow-up actions from previous management reviews;

j) Any changes that could affect the QAMS;

k) Adequacy of policy and objectives; and

l) Recommendations for improvement.

10.6.3 Review Output

The outputs from top management reviews shall include decisions and actions related to possible changes to policy, objectives, targets, and other elements of the QAMS, with the aim of promoting continuous improvement, including:

a) Improvement of the effectiveness of the QAMS;

b) Update of the risk assessment, and risk management plans;

c) Modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may affect the QAMS;

d) Resource needs; and

e) Improvement of how the effectiveness of controls is being measured.

11. IMPROVEMENT

11.1 Change Management

The organization shall establish a defined and documented quality assurance change management program to ensure that any internal or external changes that impact the organization are reviewed in relation to the QAMS. It shall identify any new critical activities that need to be included in the QAMS change management program.

11.2 Opportunities for Improvement

The organization shall monitor, evaluate, and exploit opportunities for improvement in QAMS performance and eliminate the causes of potential problems, including:

a) Ongoing monitoring of the operational landscape to identify potential problems and opportunities for improvement;

b) Determining and implementing action needed to improve quality assurance performance; and

c) Reviewing the effectiveness of the action taken to improve performance.

Actions taken shall be appropriate to the impact of the potential problems, and the organization's obligations and resource realities.

Top management shall ensure that actions are taken without undue delay to exploit opportunities for improvement. Where existing arrangements are revised and new arrangements introduced that could impact on the quality management of operations and activities, the organization shall consider the associated risks before their implementation.

The results of the reviews and actions taken shall be clearly documented and records shall be maintained. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

11.3 Continual Improvement

The organization shall continually improve the effectiveness of the QAMS through the use of the quality assurance management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.

Annex A
(informative)

A GUIDANCE ON THE USE OF THE *STANDARD*

NOTE: The additional text given in this annex is strictly informative and is provided to assist in understanding the requirements contained in clauses 5 - 11 of this *Standard*. While this information addresses and is consistent with the requirements of clauses 5 - 11, it is not intended to add to, subtract from, or in any way modify those requirements.

A.1 Introduction

Private Security Service Providers including Private Security Companies (collectively "PSCs") play an important role in protecting public, private, and not-for-profit sector clients operating in circumstances of weakened governances where the rule of law has been undermined due to human or naturally caused events. Clients from the public, private, and non-governmental organization (NGO) sectors engage a broad-range of services from PSCs in support of commercial, humanitarian, diplomatic, and military efforts, and to protect other activities, including rebuilding of infrastructure. The scope and scale of the activities of PSCs include guarding and protection of persons and objects, such as convoys, facilities, designated sites, property or other placed (whether armed or unarmed), or any other activity for which the Personnel of Companies are required to carry or operate a weapon in the performance of their duties. This *Standard* provides auditable criteria for PSCs, and their clients, to demonstrate accountability that human rights and fundamental freedoms are adhered to, and untoward, illegal, and excessive acts prevented.

The primary role of PSCs is to protect the fundamental and universal human right of people to be secure in their persons and property in conditions of weakened governance. In many parts of the world, this basic right is under attack. In many cases, these attacks are directed against people who are working to alleviate the suffering of affected populations, to restore critical infrastructure necessary for the well-being of individuals and society, or are engaged in other activities that will lead to long term stability and development of the population. These attacks may be for the purpose of immediate financial gain, politically motivated, or for reasons of hatred, bigotry, and/or revenge. These attacks not only violate the basic rights of the individuals targeted by that violence, but also affect the broader population who are consequently denied food, water, medical treatment, electricity, employment, and peace. Frequently, the perpetrators seek cover among the civilian population, using the innocent to shield themselves, often using intimidation and fear. Where the community or effective authority lacks the capacity to broadly defend lives, rights, and property of their citizens – or is incapable of providing minimum security or bringing perpetrators of this violence to justice – individuals and organizations may seek recourse to commercial providers of security services to provide the capacity for self-defense to prevent the commission of a serious offenses involving grave threat to life or serious bodily harm.

This *Standard* recognizes that PSCs operate in high-risk environments that are inherently unstable and dangerous. The *Standard* provides principles and requirements to manage risk associated with operating in regions of weakened governance, where the rule of law has been undermined by human or naturally caused events. The purpose of this *Standard* is to improve and demonstrate the 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, laws, and fundamental freedoms.

The challenge to PSCs goes beyond response and reporting of incidents. Organizations should engage in a comprehensive and systematic process to preemptively manage the risks associated with their operations. This requires the creation of an on-going, dynamic, and interactive management process that serves to promote a culture of respect for human rights, laws, and fundamental freedoms, while providing clients with a quality of service to support their mission.

The sanctity of human life is the paramount underlying principle of this *Standard*. PSCs, and their clients, have an obligation to protect the lives and safety of both internal and external stakeholders (including the community at large). By using this *Standard*, PSCs can better understand the risks they face and preemptively develop strategies that will:

a) Manage risk posed to the lives and property of those whom they are contractually obligated to protect;

b) 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;

c) Demonstrate commitment, conformance, and accountability to respect human rights, laws, and fundamental freedoms;

d) Reduce risk and support the business and operational mission; and

e) Successfully manage an undesirable or disruptive event by developing a strategy and action plans to safeguard its interest and those of its clients and other stakeholders.

Adaptive and preemptive planning and preparation for potential undesirable and disruptive events will help reduce the likelihood and consequences of an event. The holistic management process can help avoid or minimize the interruption or suspension of mission critical services and operations.

This *Standard* provides guidance or recommendations for any PSC to identify and develop best practices to assist and foster action in:

a) Reducing risks throughout its operations and supply chain (including subcontractors);

b) Providing top management driven vision and leadership for strategies to protect tangible and intangible assets while respecting human rights, laws, and fundamental freedoms;

c) Identifying and evaluating risks critical to its short- and long-term success;

d) Minimizing the likelihood and consequences of a wide variety of hazards and threats;

e) Understanding, providing , and applying training in respect for human rights;

f) Understanding the roles and responsibilities needed to protect assets and further the mission;

g) Managing incident response measures and resources;

h) Developing, testing, and maintaining incident prevention and response plans, and associated operational procedures;

i) Developing and conducting training and exercises to support and evaluate prevention, protection, preparedness, mitigation, response, recovery, and operational procedures;

j) Developing and conducting training programs to support operations requiring the use of force;

k) Developing internal and external communications procedures, including response to requests for information from the media or the public;

l) Establishing metrics for measuring and demonstrating success;

m) Documenting the key resources, infrastructure, tasks, and responsibilities required to support critical operational functions; and

n) Establishing processes that ensure the information remains secure, current, and relevant to the changing risk and operational environments.

The success of the management system depends on the commitment of all levels and functions in the organization, especially the organization’s top management. Decision makers should be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with prevention, mitigation, and management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what the roles and responsibilities of all persons working on behalf of the organization are. The *Standard* drives a culture of quality assurance within the organization where “quality” is seen as both provision of services as well as respect for human rights, laws, and fundamental freedoms.

Clients of PSCs have an inherent interest to ensure that PSCs abide by the principles of this *Standard*, given that the actions of a PSC directly reflect on their clients, particularly when the client is a government entity. The consequences of untoward, illegal, and excessive acts on the part of a PSC can range from embarrassing the client; to disrupting critical diplomatic, aid, and reconstruction efforts; and increasing the threat. Therefore, when contracting the services of PSCs, clients also have an interest in making sure that the contracts reflect the transparent implementation of a QAMS.

A.2 Human Rights and International Law

The discussion of human rights and international law in this clause is a broad summary; legal advice should be sought before conducting security operations in any particular environment.

See Annex E, *Bibliography*, for citations to some of the applicable international instruments.

A.2.1 Respect for Human Rights

Building on 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, "human rights" where it appears in this *Standard* refers to the rights and freedoms articulated in international human rights law to which all people are entitled to without discrimination. Human rights are universal and are interrelated, interdependent, inalienable, and indivisible. They are articulated in both national and international law.

For the purposes of this *Standard*, PSCs should respect all human rights, including but not limited to, non-derogable human rights, such as:

- Right to life;
- Freedom from genocide and crimes against humanity;
- Freedom from torture, cruel, inhuman, or degrading treatment or punishment;
- Freedom from slavery, slave trade, and servitude;
- Rights to due process, equal treatment before the law, and a fair trial;
- Right to be free from retroactive application of penal laws;
- Right to freedom of thought, conscience, and religion; and
- Freedom from discrimination.

The purpose of a PSC is to enable the right to life in high risk environments that are inherently unstable and dangerous, doing so in such a way that does not violate other human rights. This *Standard* recognizes the fundamental importance of self-defense to protect the right to life. Self-defense allows an individual to use reasonable force in defense of oneself or others. Deadly force should only be used in self-defense or the defense of others, when it reasonably appears necessary to prevent the commission of a serious offense involving violence threatening death or serious bodily harm.

A.2.2 International Humanitarian Law

International humanitarian law (IHL) or the *law of armed conflict (LOAC)* refers to international treaty and customary rules that govern war or armed conflict (the laws and customs of war). For the purposes of this guidance, IHL and LOAC can be considered to have the same meaning.

IHL defines the conduct and responsibilities of individuals and States during armed conflict. IHL aims to limit the suffering caused by war by protecting people who are not or are no longer taking part in hostilities, and restricting the methods and means of warfare. The essential rules of IHL include obligations to:

a) Engage in limited methods and means of warfare;
b) Distinguish between those directly participating in hostilities and the civilian population (noncombatants);
c) Limit attacks solely to military objectives;
d) Avoid unnecessary harm to the civilian population and property;
e) Abstain from harming or killing an adversary who surrenders or who can no longer take part in the fighting;
f) Treat humanely all persons taking no active part in hostilities (including adversaries who have surrendered, are wounded, or sick); and
g) Abstain from physical or mental torture or performing cruel punishments. .

International legal obligations particularly applicable to PSCs are specified in the *Montreux Document,* Part 1, paragraphs 22-27.

During an armed conflict, the personnel of PSCs are normally considered civilians under IHL. As civilians, PSC personnel may not be the object of a direct attack unless and for such time as they directly participate in hostilities. Under the conditions of this *Standard*, PSCs and their personnel are not privileged to either engage in combat or carry out any other act that is likely to directly harm the military operations or capacity of a party to the conflict. This restriction generally means that PSC personnel cannot, for example, attack enemy armed forces or defend a military objective against an attack by enemy armed forces without losing their protection as civilians. Direct participation in hostilities by PSC personnel is not prohibited by IHL. If captured, PSC personnel who are authorized to accompany the armed forces do not lose any existing entitlement to prisoner of war status as a result of their direct participation in hostilities. However, as civilians without combatant privileges, PSC personnel can be held accountable under criminal and tort law for any serious injury or death inflicted on others or destruction of property committed by them. Regardless of prisoner of war status, captured PSC personnel are entitled to adequate and humane conditions of detention.

Self-defense and the defense of others against unlawful attack is an inherent right and is not direct participation in hostilities. This right to self-defense applies even if the attacker(s) is/are members of the armed forces of a State, if such attack is unlawful under IHL. Use of force by PSC personnel to resist unlawful attacks does not forfeit their protected status as civilians. However, defensive fire against or otherwise resisting a lawful attack (e.g., by a party to the armed conflict against an enemy party's military objective) could be considered direct participation in hostilities, which would result in the loss of protected status during that action.

PSC personnel can be charged and convicted for serious violations of international law, such as war crimes and crimes against humanity. These crimes have extraterritorial jurisdiction, with varying degrees of application. Some States and international organizations promote a concept of universal jurisdiction for such crimes. Under this concept, it is possible for persons accused of such crimes to be brought to court in any country, before any judge. Directors, managers, and supervisors of PSC personnel can also be held liable for such crimes committed by personnel under their effective authority, either because of orders or instructions they issue or the failure of PSC supervisors to exercise proper control over their personnel. Companies may also be found liable under evolving criminal or tort law.

The guidance in this entire Annex is informative only; it is recommended that PSCs consult with appropriate legal counsel for interpretations and evolving law. The organization should include more comprehensive training for persons working on its behalf operating in conditions of armed conflict that includes, but may not be limited to:

a) The difference between self-defense/defense of others and direct participation in hostilities;

b) Specific individual crimes, such as torture and other inhumane treatment, that could be charged against them as war crimes or crimes against humanity;

c) Specific considerations for the use of force in international and non-international armed conflicts, to include the differences between international armed conflict and armed conflict not of an international character and the status of various belligerents and non-State armed groups;

d) The difference between Rules for the Use of Force appropriate to PSCs and other civilians and Rules of Engagement proper to Armed Forces; and

e) The circumstances in which a PSC and persons working on its behalf could be considered privileged belligerents or incorporated into Armed Forces.

A.2.3 Customary International Law

Customary international law refers to the rules of law derived from the consistent conduct of States acting out of the belief that the law required them to act that way. Elements of customary international law include widespread repetition by States of similar international acts over time (State practice), the acts occur out of a sense of obligation, and the acts are accepted by a significant number of States.

Customary international law is binding on all States regardless of whether they are a party to a particular treaty or convention. A number of human rights listed above are today considered customary international law. With regard to IHL, significant elements of the laws covering international armed conflict remain customary, rather than treaty law. The application of much of IHL to non-international armed conflicts is a matter of customary international law. Issues relating to civilian status in armed conflict and direct participation in hostilities are still emerging as matters of customary law and directly affect the activities of PSCs.

A.2.4 International Human Rights Law

International human rights law refers to the body of international law that is designed to promote and protect human rights and consists of treaties and agreements between States. International human rights law is binding on States and their agents. International human rights standards are enforceable through various international and regional courts and tribunals, as well as the UN charter and treaty-based mechanisms. The principles described in the ICoC are intended to guide PSCs in developing and implementing policies and procedures that are consistent with the objectives of international human rights law.

A.3 Management System Requirements

A management system is a dynamic and multifaceted process, with each element interacting as a structured set of functional units. It provides a framework that is based on the premise that the component parts of a system can best be understood when viewed in the context of relationships with each other and with other systems, rather than in isolation. The only way to fully understand and implement the elements of a management system is to understand that parts in relation to the whole. Therefore, it should be noted that a management system is not a simple cycle, but rather a complex set of interrelated elements interacting with each other. This results in an iterative process where establishing the context and policy, risk assessment, implementation, operation, evaluation, and review are not a series of consecutive steps, but rather a network of interacting functions.

The management systems approach is characterized by:

a) Understanding the context and environment within which the system operates;

b) Identifying the core elements of the system, as well as the system boundary;

c) Understanding the role or function of each element in the system; and

d) Understanding the dynamic interaction between elements of the system.

The systems approach ensures that holistic strategies and policies are developed. It provides a sound analytical basis for developing strategies and policies that are to be implemented in the complex and changing environment in which the organization operates. Establishing a framework for assessing the risks and effectiveness of strategies and policies prior to and during implementation provides a feedback loop for decision-making throughout the process.

The implementation of the QAMS specified by this *Standard* is intended to result in:

a) Improved service provision;

b) Security and safety of internal and external stakeholders; and

c) A culture of respect for human rights, laws, and fundamental freedoms.

Therefore, this *Standard* is based on the premise that the organization will monitor, review, and evaluate its QAMS to identify opportunities for continual improvement and the implementation of corrective and preventive measures. The rate, extent, and timescale of this continual improvement process are determined by the organization in the light of the changing risk environment, economic, and other circumstances. This *Standard* requires an organization to:

a) Establish an appropriate quality assurance management policy;

b) Assess the risks related to the organization's activities;

c) Identify applicable legal requirements and other requirements to which the organization subscribes;

d) Identify priorities and set appropriate quality assurance management objectives and targets;

e) Establish a structure and programs to implement the policy and achieve objectives and meet targets;

f) Facilitate planning, control, monitoring, preventive and corrective action, and auditing and review activities to ensure both that the policy is complied with and that the QAMS remains appropriate; and

g) Be capable of adapting to changing circumstances.

A.4 General Principles

PSCs should integrate all the principles described in clause 4 of this *Standard* into the design of its management system for the QAMS to be successful. The goal is to achieve the PSC's and client's objectives and protect assets (both tangible and intangible) while assuring human safety and security coupled with respect for human rights. Quality assurance management will depend on the effectiveness of integrating these principles into the management framework, which drives a quality assurance culture throughout all levels of the organization. Use of these principles should establish an environment where information is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

The QAMS framework provides key principles, a common language, and clear direction and guidance for decision making. Managing risks is not just the responsibility of management. For a quality assurance program to be effective, it needs to be implemented by every person working on behalf of the organization. It is a top-down, bottom-up approach. Protection of human rights and managing risk must become an integral part of the organization's culture. Therefore, all risk-makers and risk-takers should be the risk-managers.

All organizations, particularly PSCs, face a certain amount of uncertainty and risk. In order to assure sustainability of operations and maintain competitiveness and performance, organizations must have a system to manage their risks. The challenge is to assess, evaluate, and treat risk in order to cost effectively manage the risk and uncertainty while meeting the organization's, and client's, strategic and operational objectives. Given the finite resources of organizations, it is imperative that they build a robust management system to address any array of risks they may face.

A.4.1 Getting Started – Gap Analysis

An organization with no existing QAMS should establish its current position with regard to human rights protection and its capabilities to manage potential risk scenarios by means of a gap analysis. A gap analysis will enable the organization to compare its actual performance with the potential performance needed to meet its objectives. The analysis should consider the organization's risks (including potential impacts) as a basis for establishing the QAMS.

The gap analysis should cover five key areas:

1. Identification of risks, including those associated with operating conditions, emergency situations, accidents, and potential undesirable and disruptive events;
2. Human rights impact assessment;
3. Identification of applicable legal requirements and other requirements to which the organization subscribes;
4. Evaluation of existing risk management practices and procedures, including those associated with subcontracting activities; and
5. Evaluation of previous emergency situations, and accidents, as well as previous measures taken to prevent and respond to undesirable and disruptive events.

In all cases, consideration should be given to operations and functions within the organization, its relationships with its relevant stakeholders (e.g., clients, subcontractors, and the local community), and to potentially disruptive and emergency conditions. Tools and methods for undertaking a gap analysis may include checklists, conducting interviews, direct inspection and measurement, or results of previous audits or other reviews, depending on the nature of the activities.

A.5 Establishing the Framework

A.5.1 Understanding the Organization and its Context

The organization establishes the context of its QAMS by identifying and understanding the internal and external influences and environment in which it operates. By establishing the context, an organization can define the scope of its QAMS and design a fit-for-purpose framework for quality assurance management. This should help assure that the organization meets the objectives, needs, and concerns of internal and external stakeholders (e.g., clients, supply chain partners, subcontractors, local communities). The context will determine the criteria for managing the risk to the organization, clients, and impacted communities thereby providing a basis for setting risk criteria and parameters for the risk assessment and treatment processes.

External context includes:

a) Social, socio-economic, environmental, geographic, political, cultural, competitive, business, financial, supply chain, interdependencies, and community factors;
b) Key drivers and trends having impact on objectives;
c) Client and supply chain needs and requirements; and
d) Needs, interests, and perceptions of external stakeholders.

Internal context includes:

a) Policies, processes, and business mission;
b) Capabilities, resources and knowledge (people, processes, systems, technology, time, and capital);
c) Overall risk management strategy;
d) Information – systems, flows, and decision making processes;
e) Internal stakeholders;
f) Objectives and strategies of the organization;
g) Perception, values, and culture;
h) Policies and processes; and
i) Governance, roles, and accountabilities.

During the process of establishing the internal and external context, the organization should identify the significant tangible and intangible assets of the organization. This includes identifying the relative importance of various types of assets to the viability and success of the organization.

A.5.2 Supply Chain and Subcontractor Node Analysis

Supply chains and the use of subcontractors are integral parts of PSC operations. While there is significant interdependence within a supply chain, each individual node of a supply chain is unique in certain respects; this uniqueness may require unique approaches to the management of the risks involved. Therefore, to manage the risks within a supply chain, the organization needs to identify:

a) The role of organizations and individuals at each tier or level of its upstream and downstream supply chain or network;
b) Understand the interdependencies and supporting infrastructure critical to mission success;
c) How each node plays a role in adding value to the performance of other members of the chain, directly or indirectly;
d) Determine how each node has the potential to contribute to the risk profile of the organization, both positively and negatively; and

e) Evaluate how each node exerts some influence on the success of minimizing risk implementation of the management system.

When conducting node analysis, the organization should recognize the decisions taken at the individual node has potential chain-wide implications. Therefore, the risk factors throughout the supply chain need to be understood and controlled for successful implementation of the QAMS.

A.5.3 Scope of Quality Assurance Management System

An organization has the freedom to define the boundaries for implementing its QAMS. It may choose to implement the QAMS across the entire organization, specific operating units, discrete geographic locations, or clearly defined supply chain flows. These scoping boundaries reflect top management objectives for the QAMS, and the size, nature, and complexity of the organization and its activities. Once top management defines the QAMS scope, all assets, activities, products, and services within that scope become elements of concern within the QAMS.

The organization should justify all exclusions from the scope of the QAMS using the risk assessment in the justification. Exclusions may include the inability of an organization to control certain services or operations; however, exclusions do not negate the organization's responsibilities to value the sanctity of human life or its obligations to respect human rights, laws, and fundamental freedoms. The scope should ensure the integrity of the organization and its clients operations. The credibility of the QAMS depends on the choice of organizational boundaries defined in the scope.

Outsourced and subcontracted activities remain the organization's responsibility and should be within the QAMS. If an outsourced or subcontracted product, service, activity, or part of the organization's supply chain remains under the organization's risk accountability and management control, then top management should place it within the scope of the QAMS. The organization should make appropriate agreements and take appropriate measures to assure effective quality assurance management agreements are in place with its subcontractors and outsource partners.

The level of detail and complexity of the QAMS, the extent of documentation required, and resources committed to the QAMS should guide the QAMS scope statement. When the organization implements the *Standard* for a specific operating unit, then the organization may use applicable policies, plans, and procedures developed by other parts of the organization to satisfy the requirements of this *Standard*.

A.6 Leadership

A.6.1 Management Commitment

The top management of the organization (such as the managing director or chief executive) should demonstrate commitment and resolve to implement the QAMS in the organization. Without top management commitment, no management system can succeed. Top management should demonstrate to its internal and external stakeholders a visible commitment to quality assurance in the provision of security services and respect for human rights, laws, and fundamental freedoms. To initiate and sustain the QAMS effort, top management should communicate to all persons working on behalf of the organization the importance of:

a) Making organizational and individual competence in the provision of security services inherent in everything the organization does. Respect for human rights, laws, and fundamental freedoms is an integral component of all security services provided and internal operations;
b) Integrating quality assurance management throughout the organization; and
c) Looking at problems as opportunities for improvement.

The top management should provide evidence of its commitment to the development and implementation of the quality management system and continually improve its effectiveness by:

a) Communicating to the organization the importance of meeting the requirements of this *Standard*;
b) Setting and communicating the policy and risk criteria;
c) Ensuring that quality assurance objectives are established at all levels and functions;
d) Appointing one or more individuals within the organization to be responsible for the management system;
e) Ensuring that the responsibilities and authorities for relevant management system roles are assigned and communicated within the organization;
f) Allocating appropriate resources for the management system;
g) Demonstrating commitment to the management system and risk minimization;
h) Promoting awareness of risk and QAMS requirements throughout the organization;
i) Leading by example; and
j) Participating in reviews and driving the continual improvement process.

It is essential that top management of the organization sponsors, provides the necessary resources, and takes responsibility for creating, maintaining, testing, and implementing a comprehensive QAMS. This will insure that management and staff at all levels within the organization understand that the QAMS is a critical top management priority. It is equally essential that top management engage a “top down” approach to the QAMS: so that management at all levels of the organization understand accountability for system maintenance as part of the overall governance priorities.

A.6.2 Quality Assurance Management Policy

The quality assurance management policy is the driver for implementing and improving an organization's QAMS. This policy should therefore reflect the commitment of top management to:

a) The sanctity of human life and safety a first priority;
b) Avoid, prevent, and reduce the likelihood and consequences of disruptive and undesirable events;
c) Comply with applicable legal requirements and other requirements;
d) Respect human rights; and
e) Continual improvement.

The quality assurance management policy is the framework that forms the basis upon which the organization sets its objectives and targets. The quality assurance management policy should be sufficiently clear to be capable of being understood by internal and external stakeholders and should be periodically reviewed and revised to reflect changing conditions and information. Its area of application (i.e., scope) should be clearly identifiable and should reflect the unique nature, scale, and impacts of the risks of its activities, functions, products, and services.

The quality assurance management policy should be communicated to all persons who work for or on behalf of the organization, including its clients, supply chain partners, subcontractors, and relevant members of the local community. Communication to subcontractors and other external parties can be in alternative forms to the policy statement itself, such as rules, directives, and procedures. The organization's quality assurance management policy should be defined and documented by its top management within the context of the quality assurance management policy of any broader corporate body of which it is a part and with the endorsement of that body.

A quality assurance management planning team – including senior leaders from all major organizational functions and support groups – should be appointed to ensure wide-spread acceptance of the QAMS.

A.6.3 Resources, Roles, Responsibilities, and Authorities

The resources needed for the QAMS should be identified. These include human resources and specialized skills, equipment, internal infrastructure, technology, information, intelligence, and financial resources. Top management should ensure the availability of resources essential for the establishment, implementation, control, testing, and maintenance of the QAMS.

The management system is implemented by people within the organization. One or more qualified persons should be appointed and empowered to implement, test or exercise, and maintain the QAMS. Top management should conduct its own periodic reviews and audits of the overall QAMS. A quality assurance management planning team, including senior leaders from all major organizational functions and support groups may be appointed to ensure widespread acceptance of the QAMS.

A.7 Planning

A.7.1 Legal and Other Requirements

The organization should identify and understand legal, regulatory, and contractual requirements that affect the achievement of its objectives. These may include national, international, state, local, legal, and regulatory requirements. Identifying and understanding these requirements should help to ensure legal compliance, prevent litigation, minimize liability, improve the organization's image, and enhance the organization's capability to provide responsible protective services to its client.

Examples of other requirements to which the organization may subscribe include, if applicable:

a) Business and other contractual obligations;

b) Agreements with public authorities, community groups, or non-governmental organizations;

c) Agreements with clients;

d) Non-regulatory guidelines;

e) Voluntary principles or codes of practice;

f) Product or service stewardship commitments (e.g., warranties);

g) Requirements of trade associations;

h) Public commitments of the organization or its parent organization;

i) Non-binding protocols;

j) Healthcare requirements;

k) Financial obligations;

l) Social responsibility and environmental commitments; and

m) Identity information and privacy requirements.

The *Montreux Document,* Section 1, Paragraph E, summarizes the pertinent international legal obligations applicable to PSCs. Specific legal obligations vary by jurisdiction; geographic location; the type and nature of operations; and the location, type, and nature of the organization's customers. Therefore, it is important that the organization be aware of its obligations within the context of its operating environment.

The organization should identify all relevant statutory, regulatory, contractual, and other requirements and communicate this information to appropriate stakeholders. The organization should evaluate which requirements apply and where they apply, and identify who should receive this information. The organization should explicitly define, document, and keep current its approach to accessing and addressing these requirements. Similarly, the organization should define and document specific operational controls as well as individual responsibilities to meet these requirements.

A.7.2 Risk Assessment and Monitoring

PSCs operate in inherently dangerous and high risk environments. They must manage risk to the client while also managing risk to the organization and impacted communities. The organization needs to achieve its tactical, operational, and business objectives within the context of protecting life and property of its clients, people working on its behalf, and local communities while respecting human rights. Respecting rights creates value for the business, and therefore is intrinsically a business objective requiring due diligence to accomplish the operational mission while respecting human rights and adhering to local and international law. The risk assessment provides a clear understanding of the risk environment in order for the organization to make informed decisions in prioritizing its risks and their treatment.

The risk assessment process provides an understanding of the risks that could affect the organization's achievement of its operational and business objectives. It is intended to create a systematic process for an organization to identify, analyze, and evaluate risks to determine those that are significant to the organization and its stakeholders. The risk assessment provides a basis for evaluating the adequacy and effectiveness of current controls in place, as well as decisions on the most appropriate approaches to be used in managing and treating risks. It identifies those risks that should be addressed as a priority by the organization's QAMS. The risk assessment provides the foundation for setting objectives, targets and programs within the management system, as well as measuring the efficacy of the QAMS.

An organization should apply the ISO 31000:2009, *Risk Management – principles and guidelines on implementation.* (See Figure 3, based on ISO 31000:2009.)

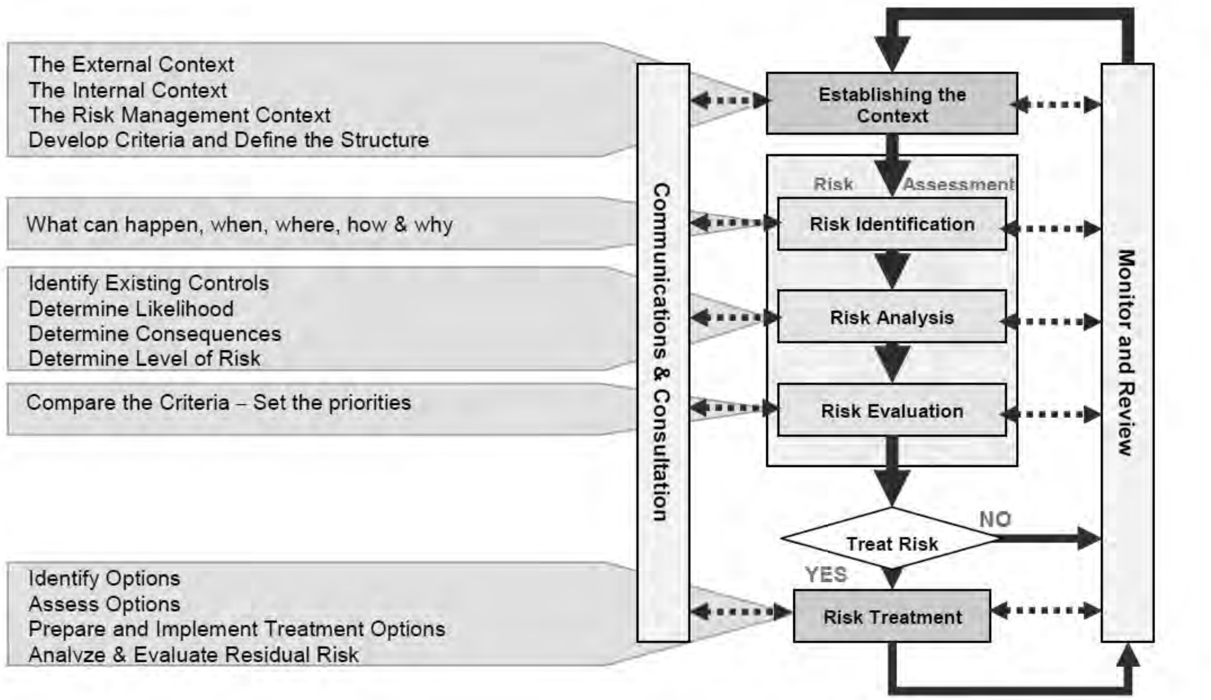
The External Context
The Internal Context
The Risk Management Context
Develop Criteria and Define the Structure
What can happen, when, where, how & why
Identify Existing Controls
Determine Likelihood
Determine Consequences
Determine Level of Risk
Compare the Criteria – Set the priorities
Identify Options
Assess Options
Prepare and Implement Treatment Options
Analvze & Evaluate Residual Risk
Communications & Consultation
Establishing the Context
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Treat Risk
NO
YES
Risk Treatment
Monitor and Review

Figure 3: Process for Managing Risk

The risk assessment process is conducted within the internal and external context of the organization. Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation:

a) *Risk Identification*: The process of identifying and documenting risks by means of threat, criticality, and vulnerability analysis. The process considers the causes and sources of risks, as well as events, situations, and circumstances that could impact the organization and its stakeholders.

   The identification should include of all sources of risk that may deter the organization from achieving its business, tactical and operational objectives, including the rights, security, and safety of clients, persons working on behalf of the organization as well as other internal and external stakeholders.

b) *Risk Analysis*: The process of developing an understanding of risk. It provides the basis for determining which risks should be treated and the most appropriate method for treating them. It considers the causes and sources of risk, their consequences, and the likelihood that the incident and associated consequences can occur.

   An organization should determine what the consequences of an event upon stakeholders will be if a threat materializes. The level of risk is a function of the likelihood and consequences and provides the basis for prioritizing the risks that need to be treated;

c) *Risk Evaluation*: The process of comparing the estimated levels of risk with the risk criteria defined when the context was established. It determines the significance of the level and type of risk. The risk evaluation uses the understanding of the risk obtained in the risk analysis to make decisions about the strategies required for risk control and treatment.

The risk assessment provides an understanding of risks, their causes, likelihood and consequences. Therefore, an organization should conduct a comprehensive risk assessment within the scope of its QAMS, taking into account the inputs and outputs (both intended and unintended) associated with:

a) Its activities, products, and services;
b) Interactions with the environment and community;
c) Relations with internal and external stakeholders (e.g., clients, subcontractors, local government); and
d) Infrastructure and interdependencies.

The risk assessment should include a detailed analysis and evaluation of the uncertainties associated with the successful achievement of the organization's mission – for example (but not limited to):

a) Tactical risks related to the mission and operations;
b) Risks related to the reputation of the organization and the client;
c) Political and social implications of the organization's activities;
d) Threats and consequences to persons working on behalf and the organization;
e) Threats and consequences to local communities and the potential impact of operations on their human rights;
f) Risks related to the use of subcontractors and interactions with other PSCs; and
g) The interrelationships between tactical and operational risks and the need to respect human life and rights.

Many methodologies exist for risk assessments. The organization should establish, implement, and maintain a formal methodology that is documented and repeatable. Assumptions, scope, evaluation criteria, and results should be clearly defined and reviewed by top management.

Since an organization might have many risks, it should establish and document criteria and a methodology to determine those that it will consider significant. There is no single method for determining significant risks. However, the method used should provide consistent results and include the establishment and application of evaluation criteria, such as those related to protection of life and human rights, criticality of activities and functions, legal issues, and the concerns of internal and external stakeholders. An organization should analyze likelihood and consequences of disruptive and undesirable events to its operations and identify critical operations that are given high priority for developing response and recovery times and objectives.

When assessing consequences the organizations should consider:

a) *Human Cost*: Physical and psychological harm to clients, persons working on its behalf, suppliers, local communities, and other stakeholders;

b) *Financial Cost*: Equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.;

c) *Image Cost*: Reputation, standing in the community, negative press, loss of clients, etc.;

d) *Indirect Impacts*: On the regional economy and reduction in the regional net economy, etc.; and

e) *Environmental Impacts*: Degradation to the quality of the environment or to endangered species.

The risk assessment is an inclusive process taking into account the input of internal and external stakeholders. The risk and impact identification, analysis, and evaluation processes are framed within the operating environment of the organization; therefore, they should take into account the internal and external context and legal and other requirements.

To achieve results that accurately reflect the risk profile of the organization, data for the risk assessment should be gathered by a competently trained team. The sampling techniques for the collection of administrative, financial, technical, and physical data should be selected to assure representative samples. The risk assessment is not an exact science: therefore, assumptions and reliability of information should be documented. All operational units of the organization within scope of the QAMS should be directly consulted during the data-gathering process. Results of the risk assessment should be reported and reviewed by top management in order to establish the quality assurance management objectives, targets, and strategies. The organization should define the scope of the risk assessment based on:

a) QAMS scope (products, services, and activities);

b) Client expectations and obligations;

c) Legal, regulatory, and contractual requirements;

d) Respect for human rights;

e) Impacted communities expectations;

f) Risk appetite;

g) Interdependencies and infrastructure requirements; and

h) Data/information requirements.

The risk assessment process should consider normal and abnormal operating conditions, as well as reasonably foreseeable disruptive situations, in order to better control disruptive and undesirable events. However, it should be kept in mind that it is not possible to foresee all disruptive and undesirable situations, so the organization should also consider the consequences of an event on critical assets, activities, and functions, as well as impacted communities, regardless of the nature of an event in order to preemptively manage its risks.

The risk assessment should:

a) Use a documented quantitative and/or qualitative methodology to estimate likelihood or probability of the identified potential risks and significance of their consequences if an event materializes;

b) Be based on reasonable and defined criteria;

c) Give due consideration to all potential risks it recognizes to its operations;

d) Consider its dependencies on others and others dependencies on the organization, including client, community, and supply chain dependencies and obligations;

e) Evaluate the consequences of legal and other obligations which govern the organization's activities;

f) Consider risks associated with stakeholders, contractors, suppliers, and other affected parties;

g) Analyze information on risks, and select those risks which may cause significant consequences and/or those risks whose consequence is hard to be determined in terms of significance;

h) Analyze and evaluate the costs, benefits, and resources needed to manage risks; and

i) Evaluate risks and impacts it can control and influence.

NOTE: It is the organization that determines the degree of control and its strategies for risk acceptance, avoidance, management, minimization, tolerance transfer, and/or treatment.

In some locations, critical infrastructure, community assets, and cultural heritage may be an important element of the surroundings in which an organization operates, and therefore should be taken into account in the understanding of its risks and impact on surroundings.

When developing information relating to its significant risks, the organization should consider the need to retain the information for historical purposes, as well as how to use it in designing and implementing its QAMS.

The process of identification and evaluation of risks should take into account the location of activities, cost and time of undertaking the analysis, and the availability of reliable data. Information already developed for business planning, regulatory, or other purposes may be used in this process.

The organization should revisit its reassessment to address changing operating conditions and in response to events. Changes that may elicit a revisit of the reassessment include changes in:

a) Contractual and industry trends;

b) Regulatory requirements;

c) Political environment;

d) Conditions due to an event; and

e) Performance based test/exercise results.

This process of identifying and evaluating risks is not intended to change or increase an organization's legal obligations.

A.7.3 Quality Assurance Objectives and Targets

Objectives and targets are established to meet the goals and commitments of the organization's quality assurance policy. By setting the quality assurance objectives and targets, the organization can translate the policy into action plans it describes in the quality assurance strategies. The objectives and targets should be specific and measureable in order to track progress and ascertain how the QAMS is performing in improving overall organizational preparedness.

Quality assurance "objectives" are overriding considerations such as minimizing accidents. Quality assurance "targets" are specific metrics for the reduction of accidents. Objectives and targets should be appropriate for the organization, based on the risk assessment. The objectives and targets should reflect what the organization does, how well it is performing, and what it wants to achieve. Appropriate levels of management should define the objectives and targets. Objectives and targets should be periodically reviewed and revised.

When the objectives and targets are set, the organization should consider establishing measurable quality assurance performance indicators. These indicators can be used as the basis for a quality assurance performance evaluation system and can provide information on the QAMS and specific prevention, mitigation, response, and recovery strategies.

In establishing its objectives and targets the organization should consider:

a) Policy commitments;
b) Alignment with strategic objectives;
c) Outcomes of the risk assessment;
d) Risk appetite and tolerance;
e) Legal and other requirements;
f) Internal and external context;
g) Performance criteria;
h) Infrastructure requirements and interdependencies;
i) Interests of stakeholders (e.g., clients, communities, and supply chain partners);
j) Technology options;
k) Financial, operational, and other organizational considerations; and
l) Actions, resources, and timescales needed to achieve objectives.

When considering its technological options, an organization should consider the use of best available technologies where economically viable, cost-effective, and judged appropriate.

The reference to the financial requirements of the organization is not intended to imply that organizations are obliged to use specific cost-accounting methodologies; however, the organization may choose to consider direct, indirect, and hidden costs.

A.7.4 Actions to Address Issues and Concerns

The quality assurance strategies and action plans are documented approaches to achieve the organization's objectives and targets. Strategies should be coordinated or integrated with other organizational plans, strategies, and budgets. Action plans may be subdivided to address specific elements of the organization's operations.

To ensure its success, the quality assurance management strategies and action plans should define:

a) Responsibilities for achieving goals (who will do it? where will it be done?);
b) Means and resources for achieving goals (how to do it?); and
c) Timeframe for achieving those goals (when will it be done?).

The strategies may be subdivided to address specific elements of the organization's operations. The organization may use several action plans as long as the key responsibilities, tactical steps, resource needs, and schedules are adequately defined in each of the documented plans.

The strategies should include – where appropriate and practical – consideration of all stages of an organization's activities related to planning, design, construction, commissioning, operation, retrofitting, production, marketing, outsourcing, and decommissioning. Strategy development may be undertaken for current activities and new activities, products, and/or services.

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

a) Removing the risk source, where possible;
b) Removing or reducing the likelihood of an event and its consequences;
c) Removing or reducing mitigating harmful consequences;
d) Sharing or transferring the risk with other parties, including risk insurance;
e) Spreading the risk across assets and functions;
f) Retaining risk by informed decision; and
g) Avoiding the risk by temporarily halting activities that give rise to the risk.

The organization's planning should take into account the priority of activities, contractual obligations, employee and neighboring community necessities, and operational continuity.

Strategies should be dynamic and monitored and modified when:

a) Outcomes of the risk assessment change;
b) Objectives and targets are modified or added;

c) Relevant legal requirements are introduced or changed;
d) Substantial progress in achieving the objectives and targets has been made (or has not been made); or
e) Activities, products, services, processes, or facilities change or other issues arise.

Determining quality assurance strategy enables the organization to evaluate a range of options. The organization may choose an appropriate approach for each activity, such that it can operate at an acceptable level. The most appropriate strategy or strategies should depend on a range of factors such as the:

a) Results of the organization's risk assessment;
b) Costs of implementing a strategy or strategies; and
c) Consequences of inaction.

The organization should minimize the likelihood of implementing a quality assurance solution that might be affected by the same event that causes a disruption.

Top management should approve documented strategies to confirm that the determination of quality assurance strategies has been properly undertaken, that they have addressed the likely causes and effects of an undesirable or disruptive event, and that the chosen strategies are appropriate to meet the organization's objectives within the organizations risk appetite.

The strategies should also consider the organization's relationships, interdependencies, and obligations with external stakeholders. These stakeholders include clients, suppliers, and outsource partners – as well as public authorities and others in the community. The organization should establish and maintain strategies that first and foremost protect life and safety of external stakeholders while respecting human rights and preserving the integrity of its delivery of products and services. In addition, interactions and coordination with public authorities and others in the community should be determined and included in strategy development. These strategic arrangements with external stakeholders should support the achievement of quality assurance objectives and be clearly defined and documented.

A.8 Structural Requirements

A.8.1 Organizational Structure

A contract provides the principal legal basis for the relationship between the client and contractor. Therefore, a clearly defined management structure is necessary to establish the roles, responsibilities, and accountability of the contract. The organization entering into a contract should be a legal entity and signatures for the organization should be clearly authorized to enter into contracts on the organization's behalf.

A.8.2 Insurance

The organization should seek insurance coverage sufficient to meet any liability for damages to any person with respect to personal injury, death, or damage to property consistent with its risk assessment. The limit of such coverage should at least be at the minimum level as prescribed by the client or recognized as best industry practice. Insurance should include employer's liability and public liability coverage. Foreign and local personnel should be provided with health and life insurance policies appropriate to their wage structure and the level of risk of their service as required by law.

When seeking insurance coverage the organization should consider:

a) The policies and limits to be held by the organization should be specified in the contract;
b) The jurisdiction of the policy and in the event of a dispute;
c) The territorial limitations;
d) Limitations of indemnity;
e) Coverage of all activities, including use of weapons;
f) Medical coverage and treatment of persons working on behalf of the organization and impacted communities;
g) Activities of subcontractors; and
h) Protection of the client.

Examples of the types of coverage to consider include (but are not limited to):

a) Liability;
b) Workers compensation;
c) Accident;
d) Property damage;
e) Kidnapping, ransom and/or captive; and
f) Keyman.

A.8.3 Outsourcing and Subcontracting

A contract should provide the legal basis for the relationship between the contractor and subcontractor. The organization is responsible for all activities outsourced to another entity. The contract should specify the responsibilities, terms, and conditions under which the subcontractor is to perform, including a clearly defined:

a) Commitment to abide by the same obligations as held by the organization and described in the *Standard*;
b) Specification of the appropriate flow-down of conformance to applicable provisions of the *Standard*;
c) Confidentiality and conflict of interest requirements;

d) Process for reporting of risks, as well as the occurrence and response to undesirable and disruptive events;

e) Definition of the support relationship between the contractor and the subcontractor; and

f) Description of the service performed by subcontractor personnel.

A.8.4 Documented Information

The level of detail of the documentation should be sufficient to describe the QAMS and how the parts work together. The documentation should also provide direction on where to obtain more detailed information on the operation of specific parts of the QAMS. This documentation may be integrated with documentation of other management systems implemented by the organization. It does not have to be in the form of a manual.

The extent of the QAMS documentation can differ from one organization to another due to the:

a) Size and type of organization and its activities, products, or services;
b) Complexity of processes and their interactions; and
c) Competence of personnel.

Examples of documents include:

a) Policy, objectives, and targets;
b) Statement of conformance;
c) Information on significant risks and impacts;
d) Procedures;
e) Process information;
f) Organizational charts;
g) Internal and external standards;
h) Incident response, mitigation, emergency, and crisis plans; and
i) Records.

Any decision to document procedures should be based on the:

a) Consequences, including those to tangible and intangible assets, of not doing so;
b) Need to demonstrate compliance with legal and with other requirements to which the organization subscribes;
c) Need to ensure that the activity is undertaken consistently; and
d) Requirements of this *Standard*.

The advantages of effective documentation include:

a) Easier implementation through communication and training;
b) Easier maintenance and revision;
c) Less risk of ambiguity and deviations; and
d) Demonstrability and visibility.

Documents originally created for purposes other than the QAMS may be used as part of this management system, and (if so used) should be referenced in the system.

A.8.4.1 Records

In addition to the records required by this *Standard*, records can include (among others):

a) Compliance records;
b) Authorization to possess weapons;
c) Accountability for serialized and sensitive equipment;
d) Reports for fuel, ammunition, and training materials;
e) Tracking of weapons, explosives, vehicles, and hazardous materials;
f) Contract compliance audit reports;
g) Export/import compliance reports;
h) Audit trail documentation;
i) Licensing;
j) Exercise and testing results;
k) Access control records; and
l) Subcontractor documentation.

A.8.4.2 Control of Documented Information

The organization should create and maintain documents in a manner sufficient to implement the QAMS. However, the primary focus of the organization should be on the effective implementation of the QAMS and on quality assurance management performance and not on a complex document control system.

Proper account should be taken of confidential information. Procedures should be established, communicated, and maintained for the handling of classified information. This information should be clearly graded and labeled to protect the:

a) Sensitivity of the information;
b) Privacy, life, and safety of individuals; and
c) Image and reputation of the client.

The organization should ensure the integrity of records by rendering them tamperproof; securely backed-up; accessible only to authorized personnel; and protected from damage, deterioration, or loss.

The organization should consult with the appropriate legal authority within their organization to determine the appropriate period of time the documents should be retained and establish, implement, and maintain the processes to effectively do so. Records should be retained for a minimum of seven years or as otherwise required or limited by law.

A.9 Operation and Implementation

A.9.1 Operational Control

An organization should evaluate those of its operations that are associated with its identified significant risks, and ensure that they are conducted in a way that will control or reduce the likelihood and adverse consequences associated with them in order to fulfill the requirements of its quality assurance management policy and meet its objectives and targets. This should include all parts of its operations including subcontractor, supply chain, and maintenance activities.

As this part of the QAMS provides direction on how to take the system requirements into day-to-day operations, it requires the use of documented procedures to control situations where the absence of documented procedures could lead to deviations from the quality assurance management policy, objectives, and targets.

To minimize the likelihood of an undesirable or disruptive event, these procedures should include administrative, operational and technological controls. Where existing arrangements are revised or new arrangements introduced that could impact on operations and activities, the organization should consider the associated minimization of threats and risks before their implementation.

A.9.1.1 Establishing Norms of Behavior and Codes of Ethical Conduct

The organization should establish, implement, and maintain a Code of Ethical Conduct for its employees, subcontractors, and outsource partners. The Code of Ethical Conduct should clearly communicate respect for human rights and the dignity of human beings (taking into account local practices and culture), as well as the prohibition of bribery, conflicts of interest, corruption, and other crimes. The Code of Ethical Conduct should ensure that all persons working on behalf of the organization understand their responsibilities to abide by human rights, local and international law, and to prevent and report any abuses of human rights including (but not limited to) prohibition of:

a) Torture or other cruel, inhuman, or degrading treatment or punishment;

b) Sexual exploitation and abuse or gender-based violence;

c) Human trafficking;

d) Slavery and forced labor;

e) The worst forms of child labor; and

f) Unlawful discrimination.

The organization should clearly communicate and provide training on the Code of Ethical Conduct to all persons working on behalf of the organization. The organization should document and maintain records of communication and training.

A.9.2 Resources, Roles, Responsibility, and Authority

The successful implementation of a QAMS calls for a commitment from all persons working for the organization or on its behalf. The roles, responsibilities, and authorities of individuals should be clearly defined to ensure implementation of the QAMS, prevent misunderstandings (particularly during an undesirable or disruptive event), and avoid missed tasks.

Management should also ensure that appropriate resources are provided to ensure that the QAMS is established, implemented, and maintained. It is also important that the key QAMS roles and responsibilities are well-defined and communicated to all persons working for or on behalf of the organization.

Roles, responsibilities, and authorities should also be defined, documented, and communicated for coordination with external stakeholders. This should include interactions with subcontractors, partners, suppliers, public authorities, and local communities. The organization should define and communicate the responsibilities and authorities of all persons engaged in quality assurance management regardless of their other roles in the organization. The resources provided by top management should enable the fulfillment of the roles and responsibilities assigned. The roles, responsibilities, and authorities should be reviewed when a change in the operational context of the organization occurs.

To demonstrate its commitment, top management should establish and communicate the organization’s QAMS policy and ensure the necessary resources for the implementation of the QAMS. Therefore, top management should designate specific management representatives with defined responsibilities and authority for implementing the QAMS, who:

a) Champions the QAMS;
b) Ensures that the QAMS is established and implemented;
c) Reports on QAMS performance over time; and
d) Works with others to modify the QAMS as needed.

It is necessary that an appropriate administrative structure be put in place to effectively deal with incident management during an undesirable or disruptive event. Clear definitions should exist for a management structure, authority for decisions, and responsibility for implementation. An organization should have an “Incident Management Team” to lead event response under the clear direction of top management or its representatives. The team should be comprised of such functions as:

a) Planning;
b) Incident response and management;
c) Human resource management;
d) Health, safety, and medical response;
e) Information management;
f) Security;
g) Legal;
h) Communications/media relations; and

i) Other critical support functions.

The Incident Management Team may be supported by as many teams as appropriate taking into account such factors as organization size and type, number of employees, location, etc. Teams should develop response plans to address various aspects of potential crises – such as damage assessment and control, communications, human resources, information technology, and administrative support. Incident response and management plans should be consistent with and included within the overall QAMS. Individuals should be recruited for membership on incident management teams based upon their skills, level of commitment, and vested interest.

A.9.2.1 Personnel

The organization should retain and train personnel with the skill, knowledge, and ability to meet its contractual obligations. All persons working on the organization's behalf should be adequately compensated and provided sufficient insurance protection corresponding with their responsibilities. Personnel, competence, and training needs are an output of the context of the organization and its contractual requirements, as well as the risk assessment and definition of objectives.

Organizations should establish procedures for the welfare of persons working on their behalf, consistent with the protections provided by applicable labor and other laws including:

a) Providing personnel a copy of any contract to which they are party to, in a language they understand;
b) Providing personnel with adequate pay and remuneration arrangements commensurate to their responsibilities and working conditions;
c) Adopting operational safety and health policies;
d) Ensuring personnel unrestricted access to their own travel documents; and
e) Preventing unlawful discrimination in employment.

The privacy and confidentiality of information about individuals should be protected. Background and operational information about individuals can be highly sensitive. It is essential that the organization establish and maintain procedures to appropriately and strictly secure the confidentiality of information both internally and externally. The organization should retain relevant documents in a secure manner for a period of time that complies with applicable laws and regulations, contractual requirements, and the organization's records policies.

At a minimum, the following information should be documented for all personnel:

a) Name, address, and contact information;
b) Contact information for immediate family and persons to notify in event of injury or death;
c) Personal identification information; and
d) Information required by legal and other requirements.

A.9.2.1.1 Uniforms and Markings

The organization should adopt and use uniforms and equipment markings that indicate the status of PSC team members and their company affiliation, using patterns, colors, or markings that are not easily confused with that of public security forces such as the military and police. Uniforms and markings selected by the organization or designated by the client may also be subject to approval by appropriate authorities in the country where the PSC operates.

Standardized uniforms and marked vehicles provide an indication to the general public, police, military, and other authorities that the PSC team members have authorization to carry and use weapons. Uniforms should include a badge number, name, or other means to distinguish individual organization personnel. Vehicle markings should include a company logo and unique number. Uniforms and other markings facilitate proper identification by the public in the event of a disruptive or undesirable event. This identification enables open and transparent reporting, and reduces the likelihood that one organization may be blamed for possible misconduct of another organization operating in the same area.

Uniforms can project a positive image about the organization and encourage professional and responsible behavior by company personnel. In situations of armed conflict, distinguishable uniforms and markings can reduce the likelihood of PSC personnel being mistaken as combatants and targeted by hostile armed forces – where these forces are abiding by IHL. To be effective, information describing the uniforms, company logo, badges, and unique vehicle markings should be made available to local authorities, the public, and – as applicable – to opposing armed forces.

Outside of conditions of armed conflict, there may be specific circumstances where a client may not wish PSC personnel to be readily identifiable as such. In other circumstances, the risk assessment may indicate that visible identification of armed security escorts will increase the threat of violence and danger to the client, the public, and security personnel. In these situations, and when a more discreet approach is consistent with local law, PSC personnel may be directed to wear other functional clothing not easily distinguishable from civilian dress, will not carry arms openly, and vehicles will not stand out from other civilian traffic. Even in discreet or low-profile situations, PSC personnel should still maintain on their persons non-transferable means of personal identification.

A.9.2.2 Selection, Background Screening, and Vetting of Personnel

The organization should establish a documented procedure for pre-employment background checks and vetting of individuals working on behalf of the organization. The organization should establish, document, implement, and maintain procedures that screen out personnel who do not meet minimum qualifications established for positions, and select appropriately qualified personnel based on their knowledge, skills, abilities, and other attributes. The screening and selection procedures should be consistent with legal, contractual requirements and the principles of the *Montreux Document* and ICoC. The screening and vetting process should be based on the nature of the job for which the candidate is being considered, the person's level of authority, and the area of specialization. The screening and vetting should take place before the candidate is offered a position and commences work. Candidates should sign appropriate authorizations and consents prior to performing background screening. A decision to retain the services of an individual should be based on the totality of the candidate's qualifications and the results of the background screening and vetting.

Wherever possible, the screening and vetting process should include:

a) Identity verification;
b) Personal history verification; and
c) Credentialing.

Exclusions should be documented when information is unavailable, unreliable, or unsuitable.

Identity verification should include verification of the validity of personal history and minimum age of the prospective employee. Personal history, validated by personal history searches when available, should consider (but not be limited to):

a) Home addresses;
b) Employment records;
c) Electronic media;
d) Criminal and civil record history;
e) Records of human rights violations;
f) Military service records;
g) Motor vehicle records;
h) Credit reports;
i) Sexual offender indices;
j) Government and industry sanctions lists; and
k) Industry specific licensing records.

Credentialing involves verifying the experience and qualifications that are presented by the candidate. The organization should look for unexplained gaps. Credentialing provides information on, but is not limited to:

a) Education verification;
b) Employment verification;
c) Licensure/certification/registration verification;
d) Personal references;
e) Supervisor and coworker interviews; and
f) Military history verification.

The organization should also establish clearly defined criteria for the screening and vetting of individuals based on:

a) Substance abuse;
b) Physical and mental fitness for activities;

c) Unsuitability to carry weapons; and
d) Ability to operate in stressful and adverse conditions.

The privacy and confidentiality of information about individuals should be protected. Personal documents, such as passports, licenses, and original birth certificates should be returned to personnel within a reasonable timeframe.

A.9.2.3 Selection, Background Screening, and Vetting of Subcontractors

The organization should only retain the services, on a temporary or continuing basis, of competent subcontractors capable of operating in a manner consistent with this *Standard* and the principles of the *Montreux Document* and ICoC. The organization is responsible and liable for the subcontractor's work. The organization should establish, maintain, and document clearly defined criteria for the screening and vetting of subcontractors to be used in contracting. Contractual agreements with subcontractors should be documented and retained in accordance with applicable laws and contractual obligations with the client.

Criteria for subcontracting should include the subcontractor's capacity to:

a) Meet the requirements of this *Standard*;
b) Carry out its activities in compliance with relevant laws (local, national, humanitarian and human rights);
c) Protect the image and reputation of the client;
d) Provide adequate resources and expertise, including competent personnel, to meet operational objectives;
e) Ensure transparency, accountability, and appropriate supervision in the implementation of assigned duties;
f) Take into account the financial and economic obligations (including appropriate remuneration of their personal and insurance coverage);
g) Obtain requisite registrations, licenses, or authorizations;
h) Maintain accurate and up to date personnel and property records; and
i) Acquire, use, return, and dispose of weapons and ammunition in accordance with applicable laws and contractual obligations.

A.9.2.4 Financial and Administrative Procedures

It is necessary that the organization put in place appropriate administrative and financial structures to effectively support the QAMS, before, during, and after an undesirable or disruptive event. Procedures should be established and documented to ensure transparency with regard to authorizations, consistent with generally accepted accounting procedures and industry good practices. Therefore, a management structure, authorities, and responsibility delegation for decision-making – including spending limitations, authorities, and responsibility for implementation – should be clearly defined.

A.9.3 Competence, Training, and Awareness

The organization should identify the awareness, knowledge, understanding, and skills needed by any person with the responsibility and authority to perform tasks on its behalf. The organization should establish training and awareness programs for internal and external stakeholders who may be affected by an undesirable or disruptive event. The organization should require that subcontractors working on its behalf are able to demonstrate that their employees have the requisite competence and/or appropriate training. Management should determine the level of experience, competence, and training necessary to ensure the capability of personnel having documented responsibility for carrying out specialized QAMS management activities. Monitoring and reassessing the level of training should be conducted on an ongoing basis to identify opportunities for improvement.

It is the organization's responsibility that all persons working on behalf of the organization are sufficiently trained, both prior to any deployment and on an ongoing basis, in the performance of their functions and to respect relevant local, national, and humanitarian and human rights laws. Defined training objectives should be based on the risk assessment and facilitate uniformity and standardization of training requirements. Training should specifically include training on the:

a) Prohibition of torture or other cruel, inhuman, or degrading treatment;
b) Prohibition and awareness of sexual exploitation and abuse- or gender-based violence; and
c) Recognition and prevention of human trafficking and slavery.

The organization should identify and assess any differences between the competence needed to perform a quality assurance activity and that possessed by the individual required to perform the activity. This difference can be rectified through additional education, training, or skills development program which may include the following steps:

a) Identification of competence and training needs;
b) Design and development of a training plan to address defined competence and training needs;
c) Selection of suitable methods and materials;
d) Verification of conformity with QAMS training requirements;
e) Training of target groups;
f) Documentation and monitoring of training received;
g) Evaluation of training received against defined training needs and requirements; and
h) Improvement of the training program, as needed.

Training may include general and task- and context-specific topics, preparing personnel for performance under the specific contract and in the specific environment. General topics include, but are not limited to:

a) Rules on the use of force and firearms;
b) Humanitarian law and human rights law;

c) Religious, gender, and cultural issues, and respect for the local population;
d) Handling complaints by the civilian population: in particular, by transmitting them to the appropriate authority; and
e) Measures against bribery, corruption, and other related crimes.

Examples of task and context specific topics may include:

a) Tactical driving;
b) Interview techniques;
c) Land navigation;
d) Electronic communications
e) Medical aid;
f) Casualty evacuation; or
g) Other specified and implied tasks under the terms of the contract or services offered by the organization.

The organization should use practical, scenario-driven training that will require persons trained to make decisions in situations that reflect conditions that may be faced by security personnel in the performance of their missions, and will require them to react to the consequences of those decisions. IHL training should be structured to meet the specific conditions faced by PSCs in conditions of armed conflict. Training will focus on the civilian status of the PSC, the consequences of activities that would result in a loss of that status, and individual liability for violations of the IHL or international human rights law.

A training and awareness program may include:

a) A consultation process with staff throughout the organization concerning the implementation of the quality assurance management program;
b) Discussion of quality assurance management in the organization's newsletters, briefings, induction program, or journals (including new employee orientation);
c) Inclusion of quality assurance management on relevant web pages or intranets;
d) Online training modules housed in the organization's learning management system;
e) Learning from internal and external incidents through after action reports;
f) Quality assurance management as an item at management team meetings;
g) Conferences and classroom training; and
h) First aid and other hands-on training.

All personnel should receive training to perform their individual QAMS-related responsibilities. They should receive briefs and training on the key components of the QAMS, as well as the human rights, humanitarian law, and relevant criminal law that affect their activities directly. Such training could include procedures for prevention and mitigation measures, response, documentation and accountability requirements, the handling of local community, client, and media inquiries.

Weapons training, including less lethal weapons, should be conducted to a written standard appropriate to the weapon and the expected conditions of use. Training should include instruction, scenario-based training, mechanical training – to include weapons malfunctions and live fire qualification. Initial training should be repeated at regular intervals, not less than annually, or more frequently if required by contract of statute.

Event response teams should receive education and training about their responsibilities and duties, including interactions with first responders and other internal and external stakeholders. Team members should be trained at regular intervals (at least annually). New members should be trained when they join the organization. These teams should also receive training on prevention of undesirable events. The organization should include relevant external stakeholders and resources in their competence, awareness, and training programs.

A.9.4 Communication

Arrangements should be made for communication and consultation, internally and externally, during normal and abnormal conditions. Effective communication is one of the most important ingredients in preventing, managing, and reporting an undesirable or disruptive event. Proactive communications and consultation planning should be conducted with internal and external stakeholders in order to convey day-to-day, alert, disruptive event, and organizational and community response information. To provide the best communications and suitable messages for various groups, it may be appropriate to segment the audiences. In this way, messages may be tailored that can be released to specific groups such as employees, clients, the local community, or the media.

The communication and consultation procedures and processes should consider:

a) Internal communication between the various levels and activities of the organization and with subcontractors, clients, and partner entities;
b) Receiving, documenting, and responding to relevant communications from external stakeholders (including local communities);
c) Proactive planning of communications with external stakeholders (including the media);
d) Preemptive communication of response and reporting plans to applicable stakeholders facilitating communication and assuring stakeholders that proper planning is in place;
e) Facilitating structured communication with emergency responders; and
f) Availability of the communication channels during a disruptive situation.

Operational communication plans are necessary to provide adequate control, coordination, and visibility over ongoing security operations. Such plans should include a description of how relevant threat information will be shared between PSC personnel, military forces, and law enforcement authorities, and how appropriate assistance will be provided to PSC personnel who become engaged in hostile situations. Information should be exchanged in a way that can be understood at each level of performance, with the client or other people that are protected by the organization, and with military or other public security forces encountered by the organization's security teams.

The organization should implement a procedure for receiving, documenting, and responding to relevant communications from stakeholders and interested parties, both internal and external. This procedure can include a dialogue with interested parties and consideration of their relevant concerns. In some circumstances, responses to concerns of interested parties may include relevant information about the risks and impacts associated with the organization's activities and operations. These procedures should also address necessary communications with public authorities regarding emergency planning and other relevant issues.

A.9.4.1 Risk Communication

The organization should also identify and establish relationships with the community, public sector agencies, organizations, and officials responsible for intelligence, warnings, prevention, response, and recovery related to potential undesirable and disruptive events. The organization should formally plan its prevention, mitigation, and response communications strategy, taking into account the decisions made specific to relevant target groups, the appropriate messages and subjects, and the choice of means. When considering communication about hazards, threats, risks, impacts, and control procedures, organizations should take into consideration the views and information needs of all stakeholders, as well as the sensitivity of information.

The organization should establish procedures to communicate and consult with internal and external stakeholders specific to its risks, their impacts, and control procedures. These procedures should consider the specific stakeholder group, the type of information to be communicated, the type of disruptive event and its consequences, the availability of methods of communication, and the individual circumstances of the organization. Methods for external communication can include:

a) News or press releases;
b) Media;
c) Financial reports;
d) Newsletters;
e) Websites;
f) Phone calls, emails, and text messages (manually delivered and/or via automated emergency notification systems);
g) Voice mails; and
h) Community meetings.

The organization should conduct preplanning of communication for a disruptive event. Draft message templates, scripts, and statements can be crafted in advance for threats identified in the risk assessment, for distribution to one or more stakeholder groups identified in the risk assessment. Procedures to ensure that communications can be distributed on short notice should also be established.

The organization should designate and publicize the name of a primary spokesperson (with back-ups identified) who should manage/disseminate crisis communications to the media and others. These individuals should receive training in media relations in preparation for a crisis, and on an ongoing basis. All information should be funneled through a single team to assure the consistency of messages. Top management should stress that all organization personnel should be informed quickly regarding where to refer calls from the media and that only authorized company spokespeople may speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

A.9.4.2 Communicating Complaint and Grievance Procedures

The organization should establish and communicate to relevant stakeholders internal and external complaints and grievances procedures. The procedures should assure privacy and confidentiality and be tailored to the culture, language, education, and technology requirements of the target audience. Procedures should be established for creating a reporting mechanism for anonymous and non-anonymous complaints and grievances.

A.9.4.3 Whistleblower Policy

Whistleblowing occurs when a person working on behalf of the organization raises a concern about danger, unethical conduct, or illegality that affects others, internally or externally. Persons working on the organization's behalf may be fearful that raising the alarm will lead to retribution from their colleagues or employer. However, the organization should encourage persons working on its behalf to voice their concerns over malpractice and inappropriate acts against any internal or external stakeholder. A whistleblower policy will help the organization deal with a concern internally and in an appropriate manner, rather than publicly, causing potential damage to the organization and its client. A whistleblower policy can also serve as a as a deterrent to those who may be considering an illegal, improper, or unethical practice. A good whistleblower policy will help the organization to reduce problems and improve working conditions and operational effectiveness.

Effective whistleblower policies provide individuals with an alternative route other than their direct line management through which to raise their concerns. Therefore, organizations should establish and communicate a whistleblower policy that provides for a clear internal mechanism for anonymously reporting non-conformances and concerns about danger, unethical conduct, or illegality that affects others, internally or externally. The policy should also designate circumstances and conditions where external disclosures are acceptable and protected. Whistleblowers should receive protection for raising concerns so long as they have acted in good faith and have reasonable grounds for raising a concern.

A.9.5 Prevention and Management of Undesirable or Disruptive Events

A.9.5.1 Respect for Human Rights

Organizations are obliged to respect and comply with IHL, and human rights law imposed upon them by applicable national law, as well as international human rights standards. They should establish, implement, and document procedures to protect the sanctity of life and treat all persons humanely. Procedures should be established and communicated to appropriate parties to report and remediate any non-compliances and non-conformances.

A.9.5.2 Procurement and Management of Weapons, Hazardous Materials, and Munitions

The organization should establish, maintain, and document procedures that ensure it:

a) Acquires its munitions and equipment, in particular its weapons, lawfully;

b) Can identify and account for all ammunition;

c) Uses munitions and equipment, in particular weapons, that are not prohibited by international law;

d) Sets criteria for the use of equipment, materials, and weapons, appropriate for the task and operations, within the context of use for self-defense or the defense of others;

e) Establishes a system of traceability for equipment, materials, and weapons;

f) Creates appropriate provision for the secure storage, issue, maintenance, and use of equipment, materials, and weapons; and

g) Has complied with contractual provisions concerning return and/or disposition of weapons and ammunition.

Possession and use of weapons should be authorized by the organization, and its subcontractors, as specified in the contract. For persons working on behalf of the organization, there should be a record of:

a) Proof of authorization to carry weapons;

b) A current record of weapons training, qualification, and competence;

c) Weapons maintenance; and

d) Weapons usage.

A.9.5.3 Rules for Use of Force and Use of Force Training

The authorization to carry weapons should be issued only to qualified personnel in accordance with the terms and conditions of a contract or if there is a reasonable expectation that life or assets will be jeopardized if weapons are not carried, and carriage of weapons is in accordance with host country law. Evaluation of the necessity to carry a weapon should be made considering this expectation weighed against the possible consequences of accidental or indiscriminate use of weapons. Weapons should be issued only after the background and qualifications of personnel establish the individual has been trained and certified on the use of the specific weapon issued. Personnel should be briefed, and understand the limitations on the use of force, and that the authorization to possess weapons and ammunition may be revoked for noncompliance with established rules for the use of force.

Use of force should be reasonably necessary, proportional, and lawful. Rules for the use of force should be approved by a legal authority competent for the area in which non-lethal, less-lethal, and lethal force is to be used, considering the local context and legal requirements. Rules for the use of force should be agreed upon between the organization and the client. In establishing the rules for the use of force, the organization should:

a) Provide parameters for use of physical force;
b) Specify the circumstances under which persons are authorized to carry weapons, and prescribe the types of weapons and ammunition permitted;
c) Ensure that weapons are used only in appropriate circumstances and in a manner likely to decrease the risk of unnecessary harm;
d) Prohibit the use of those weapons and ammunition that cause unwarranted injury or present an unwarranted risk;
e) Regulate the control, storage, and issuing of weapons, including procedures for ensuring that persons are accountable for the firearms and ammunition issued to them;
f) Graduated response or an escalation of force;
g) Provide for warnings to be given, if appropriate, when weapons are to be discharged; and
h) Provide for a system of reporting whenever persons working on behalf of the organization use weapons in the performance of their duty.

Rules for use of force should be in training programs and communicated to persons working on behalf of the organization at a level appropriate to the target audience. Training should include awareness training as to the consequences of nonconformance with the rules for use of force. Records of training and demonstration of competence should be maintained.

Use of force training should emphasize:

a) Use of lethal force is used in circumstances of self-defense or defense of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life;
b) Force is to be used only as a last resort;
c) Force should be reasonably necessary;
d) Force should be reasonable in intensity, duration, and magnitude based on totality of circumstances to counter the threat; and
e) If force is required, non-lethal and less-lethal force are permissible if reasonable.

The organization should establish and provide training on a use of force continuum. At a minimum, the continuum, or the graduated use of force should include, but not limited to:

a) *Personnel Presence*—Presence as deterrence;
b) *Verbalization*—Force is not-physical; shouting of verbal warnings to desist activities;
c) *Empty-hand Control*— Use of bodily force to gain control of a situation, physically restrain, block access or detain the adversary;
d) *Less-lethal Methods*— Use less-lethal technologies to gain control of a situation;
e) *Threat of Lethal Force*—Showing a weapon and demonstrate the intent to use it; and

f) *Lethal Force*— Use of lethal weapons to gain control of a situation. Shoot to remove the threat only where necessary. Fire only aimed shots and with due regard for the safety of bystanders.

Delay of force, or sequential increase of force, is not required to resolve a situation or threat. However, persons working on behalf of the PSC should attempt to deescalate applied force if the situation and circumstances permit. Persons working on behalf of the PSC should warn adversaries and give them the opportunity to withdraw or cease threatening actions when the situation or circumstances permit.

Persons working on behalf of the organization should use reasonable force when force is used to accomplish lawful objectives. Deadly force is justified only under conditions of extreme necessity, and as a last resort when all lesser means have failed or cannot reasonably be employed. Deadly force should only be used in self-defense or the defense of others, or when it reasonably appears necessary to prevent the commission of a serious offense involving grave threat to life or serious bodily harm. The defense of others may include the use of deadly force when it is reasonably necessary to prevent the actual theft or sabotage of inherently dangerous property, the loss or destruction of which would present an imminent threat of death or serious bodily harm. Competent legal authority may also authorize the use of deadly force if it reasonably appears to be necessary to prevent the sabotage or destruction of critical infrastructure (e.g., essential public utilities and facilities), which are vital to public health or safety, and the damage to which would create an imminent threat of death or serious bodily harm or injury.

A.9.5.4 Apprehension of Adversaries

The organization should provide training in the apprehension of persons detained or captured in the course of executing the terms of the contract. This is normally limited to persons captured following an attack against the organization’s personnel, or against clients or property under the organization’s protection. This training should consist of theoretical and practical training, and emphasize protecting persons and property from further attack, while treating apprehended persons humanely. Training will include measures for protecting the apprehended person from attack or violence, reporting to the client and proper authorities, and transferring apprehended persons to competent authority at the earliest opportunity. The organization should document the transfer of custody including the apprehended person’s identity, alleged offense, and to whom the individual was transferred.

A.9.5.5 Search of Persons Detained or Apprehended

The organization should establish standardized procedures for searching personnel that are consistent with the dignity and humane treatment of persons being searched while assuring the safety of clients, property under protection, and the safety of organization personnel and bystanders. Training will distinguish between minimally invasive searches of persons at static guard posts and the comprehensive searches required after apprehension.

A.9.5.6 First Aid and Casualty Care

All personnel should receive initial and recurrent training in first aid and casualty care, with special emphasis on immediate response to traumatic injury following an attack or accident. Training should be conducted to an accepted standard. Minimally, training should include casualty stabilization, preparation, and request for evacuation. Training should also include prioritizing casualties for treatment based on severity of injury, without regard for friendly/enemy status, race, ethnic background, or other discrimination. The organization should ensure that individuals and security teams are equipped with the materials necessary to provide immediate treatment and stabilization of survivable traumatic injuries while awaiting casualty evacuation.

A.9.5.7 Occupational Health and Safety

The organization should provide a safe and healthy working environment, recognizing the possible inherent dangers and limitations presented by the local environment. Reasonable precautions should be taken to protect all persons working on behalf of the organization – or those in their care – in high-risk or life-threatening situations.

A.9.5.8 Incident Management

It is the responsibility of each organization to develop incident prevention, preparedness, mitigation response, and recovery procedures that address its needs as elucidated by the risk assessment. In developing its procedures, the organization should include consideration of:

a) Safeguarding life and assuring the safety of internal and external stakeholders is the top priority.

b) Respect for human rights and human dignity.

c) The risk assessment should be used to identify the specifics of potential disruptive events, including any precursors and warning signs.

d) Risk management should be a systematic and holistic process that builds on the formal risk assessment to identify, measure, quantify, and evaluate risks to provide the optimal solution.

e) Risk treatment options can include avoidance, elimination, reduction, spreading, transfer, and acceptance strategies:

   1) *Avoidance* and *elimination* can either evade activities that gives rise to the risk or remove the source of the risk.

   2) *Reduction* lowers the risk or the severity of the loss.

   3) *Spreading* distributes assets and/or the potential loss of capacity.

   4) *Transfer* involves sharing the risk with another party or parties.

   5) *Acceptance* is an informed decision to take a particular risk.

f) Notification of appropriate authorities and stakeholders.

The organization should establish procedures to recognize when specific dangers are noticeable that necessitate the need for some level of reaction to avoid, prevent, mitigate, or respond to the potential of the undesirable event. A strong program of detection and avoidance policies and procedures should support this process.

A potential disruptive incident, once recognized, should be immediately reported to the designated authorities, a member of management, or another individual tasked with the responsibility of crisis notification and management internally and with external stakeholders. Specific notification criteria should be established, documented, and adhered to.

Problem assessment (an evaluative process of decision making that will determine the nature of the issue to be addressed) and *severity assessment* (the process of determining the severity of the disruption and what any associated consequences) should be made at the outset of an undesirable event. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation on the organization and its stakeholders (e.g., local community and clients).

Prevention can include proactive steps to coordinate with internal and external stakeholders. Organizational culture, operational plans, and management objectives should motivate individuals to feel personally responsible for prevention, avoidance, deterrence, and detection. Cost-effective mitigation strategies should be employed to prevent or lessen the consequences of potential events. The various resources that would contribute to the mitigation process should be identified.

Preparedness and response plans should be developed around a realistic "worst case scenario," with the understanding that the response can be scaled appropriately to match the actual crisis. Considerations include:

a) People are the most important aspect of any preparedness and response plan;
b) How an organization's human resources are managed will impact the success or failure of incident management;
c) Logistical decisions made in advance will impact the success or failure of a good preparedness and response plan; and
d) Existing funding and insurance policies should be examined.

The organization should establish documented procedures that detail how the organization will manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

A.9.5.9 Incident Monitoring, Reporting, and Investigations

The organization should establish procedures for incident reporting, documenting any incident involving persons working on its behalf that involves the use of any weapon under any circumstance (except authorized training), any escalation of force, damage to equipment, injury to persons, destruction of property, attacks, criminal acts, traffic accidents, incidents involving other security forces, and any other such reporting as otherwise required by the client. The organization should establish procedures for an internal inquiry in order to determine the following:

a) Time and location of the incident;
b) Identity of any persons involved including their addresses and other contact details;
c) Injuries/damage sustained;
d) Circumstances leading up to the incident;
e) Any measures taken by the organization in response to the incident;
f) Causes of internal and external casualties;
g) Notification of appropriate authorities;
h) Identification of root causes; and
i) Corrective and preventive actions taken.

Upon completion of the inquiry, the organization should produce in writing an incident report including the above information, copies of which should be provide to appropriate stakeholders (e.g., clients and jurisdictional authorities).

Persons working on behalf of the organization should be aware of the responsibilities and mechanisms for incident reporting, including evidence gathering and preservation. The incident reporting program should be included in the organization's training program.

A.9.5.10 Internal and External Complaint and Grievance Procedures

The organization should establish a complaint and grievance procedure whereby any internal or external stakeholder who believes there are potential or actual nonconformance's with this *Standard*, or violations of international law, local laws, or human rights may file a grievance. The procedure should state that the organization, or persons working on its behalf, may not retaliate against anyone who files a grievance or cooperates in the investigation of a grievance.

Complaint and grievance procedures are not for merely documenting grievances; they should be designed to resolve disputes by identifying root causes, improving accountability, and driving a culture of continual improvement. Once a complaint or grievance has been verified, corrective and preventive actions should be implemented in an expedited fashion.

When developing complaint and grievance procedures, one or more individuals should be designated with the authority to coordinate the efforts to investigate and resolve any complaints that the organization receives alleging any actions that threaten human life, rights, or safety, or are not in conformance with the requirements of the *Standard*, or as required by the client. The organization should adopt and publish its grievance procedures providing for prompt and equitable resolution of complaints.

The procedures should include, but are not limited to:

a) Mechanisms for submission of the complaint or grievance;

b) Information requirements of the submitter, including submission of corroborating information;
c) Timeframes for submission, investigations, and outcomes;
d) Provisions for confidentiality and privacy;
e) Hierarchical steps for the resolution process;
f) Investigation procedures, both internal and external;
g) Maintenance requirements of files and records related to the grievance and investigation;
h) Disciplinary actions;
i) Steps for resolution of complaint or grievance, including actions to prevent a recurrence;
j) Documentation and communication of outcomes; and
k) Notification to appropriate authorities.

A.10 Performance Evaluation

A.10.1 Monitoring and Measurement

Performance evaluation involves the measurement, monitoring, and evaluation of the organization's quality assurance, legal compliance, and human rights performance. The organization should have a systematic approach for measuring and monitoring its quality assurance performance on a regular basis. Metrics assure the organizations policy, objectives, and targets are achieved, as well as elucidate areas for improvement.

In order to measure and monitor the organization's quality assurance performance, a set of performance indicators should be developed to measure both the management systems and its outcomes. Measurements can be either quantitative or qualitative, directly related to the risk assessment and quality assurance objectives and targets. Performance indicators can be management, operational, or economic indicators. Indicators should provide useful information to identify both successes and areas requiring correction or improvement.

The QAMS should provide procedures for defining metrics, collection of data, and analysis of data collected. Metrics should be established to monitor and measure the effectiveness of the QAMS, and identify areas for improvements to enhance performance to preemptively prevent potential undesirable and disruptive events. Knowledge gained from this information can be used to implement corrective and preventive action.

Key characteristics are those that the organization needs to consider to determine how it is managing its significant risks, achieving objectives and targets, and improving quality assurance performance.

When necessary to ensure valid results, measuring equipment should be calibrated or verified at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards. Where no such standards exist, the basis used for calibration should be recorded.

A.10.2 Evaluation of Compliance

The organization should be able to demonstrate that it has evaluated compliance with the legal and human rights requirements identified, including applicable permits or licenses.

The organization should be able to demonstrate that it has evaluated compliance with the other identified requirements to which it has subscribed.

A.10.3 Exercises and Testing

Exercising and testing scenarios should be designed using the events identified in the risk assessment. Exercising and testing can serve as an effective training tool, and can be used to validate the assumptions and conclusion of the risk assessment.

Exercising ensures that technology resources function as planned, and that persons working on the organizations behalf are adequately trained in their use and operation. Exercising can keep persons working on the organizations behalf effective in their duties, clarify their roles, and identify areas for improvement in the QAMS, its plans, and its procedures. Exercising can reveal weaknesses in the QAMS that should be corrected. A commitment to exercising lends credibility and authority to the QAMS.

The first step in exercises and testing should be the setting of goals and expectations. A critical goal is to determine whether certain prevention and response processes work and how they can be improved. The organization should use exercises and the documented results of exercises to ensure the effectiveness and readiness of the QAMS – specifically, its quality assurance plans, team readiness, and facilities – to perform and validate its quality assurance function.

Benefits of exercising and testing include:

a) Validation of planning scope, assumptions, and strategies;
b) Examine and improve competence of persons working on behalf of the organization;
c) Capacity testing (e.g., the capacity of a call-in or call-out phone system);
d) Increase efficiency and reduce the time necessary for accomplishment of a process (e.g., using repeated drills to shorten response times); and
e) Awareness and knowledge for internal and external stakeholders about the QAMS and their roles.

The organization should design exercise scenarios to evaluate the quality assurance plans. An exercise schedule and timeline for periodically exercising the QAMS and its components should be established. Exercising and testing should be realistic, evaluate the capabilities and capacities of quality assurance management, and assure the protection of people and assets involved. The scope and detail of the exercises should mature based on the organization's experience, resources, and capabilities. Early tests may include checklists, simple exercises, and small components of the QAMS. Examples of increasing maturity of exercises include:

a) *Orientation*: Introductory, overview, or education session;
b) *Table Top*: Practical or simulated exercise presented in a narrative format;

c) *Functional*: Walk-through or specialized exercise simulating a scenario as realistically as possible in a controlled environment; and
d) *Full Scale*: Live or real-life exercise simulating a real-time, real-life scenario.

There are several roles that exercise participants may fill. All participants should understand their roles in the exercise. The exercise should involve all organizational participants defined by the scope of the exercise; where appropriate, external stakeholders may be included. As part of the exercise, a review should be scheduled with all participants to discuss issues and lessons learned. This information should be documented in a formal exercise report which should be reviewed by top management. Updates should be made to plans and procedures, and corrective and preventive measures expeditiously implemented.

Design of tests and exercise should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the QAMS, personnel turnover, actual incidents, and results from previous exercises. Lessons learned from exercises and tests, as well as actual incidents experienced, should be built into future exercises and test planning for the QAMS.

Exercise and test results should be documented and retained as records.

A.10.4 Nonconformities, Corrective and Preventive Action

The organization should establish effective procedures to ensure that non-fulfillment of a requirement, inadequacies in planning approach, incidents, near misses, and weaknesses associated with the QAMS (its plans and procedures) are identified and communicated in a timely manner to prevent further occurrence of the situation, as well as to identify and address root causes. The procedures should enable ongoing detection, analysis, and elimination of actual and potential causes of nonconformities.

An investigation should be conducted of the root cause(s) of any identified nonconformity in order to develop a corrective action plan for immediately addressing the problem to mitigate any consequences, make changes needed to correct the situation and to restore normal operations, and take steps to prevent the problem from recurring by eliminating cause(s). The nature and timing of actions should be appropriate to the scale and nature of the nonconformity and its potential consequences.

Sometimes, a potential problem may be identified, but no actual nonconformity exists. In this case, a preventive action should be taken using a similar approach. Potential problems can be extrapolated from corrective actions for actual nonconformities, identified during the internal QAMS audit process, analysis of industry trends and events, or identified during exercise and testing. Identification of potential nonconformities can also be made part of routine responsibilities of persons aware of the importance of noting and communicating potential or actual problems.

Establishing procedures for addressing actual and potential nonconformities and for taking corrective and preventive actions on an ongoing basis helps to ensure reliability and effectiveness of the QAMS. The procedures should define responsibilities, authority, and steps to be taken in planning and carrying out corrective and preventive action. Top management should ensure that corrective and preventive actions have been implemented and that there is systematic follow-up to evaluate their effectiveness.

Corrective and preventive actions that result in changes to the QAMS should be reflected in the documentation, as well as trigger a revisit of the risk assessment related to the changes to the system to evaluate the effect on plans, procedures, and training needs. Changes should be communicated to affected stakeholders.

A.10.4.1 Corrective Action

The organization should take action to eliminate the cause of nonconformities associated with the implementation and operation of the QAMS to prevent their recurrence. The documented procedures for corrective action should define requirements for:

a) Identifying any nonconformities;
b) Determining the causes of nonconformities;
c) Evaluating the need for actions to ensure that nonconformities do not recur;
d) Determining and implementing the corrective action needed;
e) Recording the results of action taken; and
f) Reviewing the corrective action taken and the results of that action.

A.10.4.2 Preventive Action

The organization should take action to prevent potential nonconformities from occurring. Preventive actions taken should be appropriate to the potential impact of nonconformities.

The documented procedure for preventive action should define requirements for:

a) Identifying potential nonconformities and their causes;
b) Determining and implementing preventive action needed;
c) Recording results of action taken;
d) Reviewing preventive action taken;
e) Identifying changed risks and ensuring that attention is focused on significantly changed risks;
f) Ensuring that all those who need to know are informed of the non-conformity and preventive action put in place; and
g) The priority of preventive actions based on results of risk assessments.

A.10.5 Internal Audit

It is essential to conduct internal audits of the QAMS to ensure that the QAMS is achieving its objectives, that it conforms to its planned arrangements, that it has been properly implemented and maintained, and to identify opportunities for improvement. Internal audits of the QAMS should be conducted at planned intervals to determine and provide information to top management on appropriateness and effectiveness of the QAMS, as well as to provide a basis for setting objectives for continual improvement of QAMS performance.

The organization should establish an audit program (see ISO 19011:2011 for guidance) to direct the planning and conduct of audits, and identify the audits needed to meet the program objectives. The program should be based on the nature of the organization's activities, in terms of its risk assessment, the results of past audits, and other relevant factors.

An internal audit program should be based on the full scope of the QAMS; however, each audit need not cover the entire system at once. Audits may be divided into smaller parts, so long as the audit program ensures that all organizational units, activities, and system elements – and the full scope of the QAMS – are audited in the audit program within the auditing period designated by the organization.

The results of an internal QAMS audit can be provided in the form of a report, and used to correct or prevent specific nonconformities and provide input to the conduct of the management review.

Internal audits of the QAMS can be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence can be demonstrated by an auditor being free from responsibility for the activity being audited.

> NOTE: If an organization wishes to combine audits of its QAMS with security, resilience, safety, or environmental audits, the intent and scope of each should be clearly defined. Third-party conformity assessment, performed by a body that is independent of the organization, provides confidence to internal and external stakeholders that the requirements of this *Standard* are being met. The value of certification is the degree of public confidence and trust that is established by an impartial and competent external assessment.

A.10.6 Management Review

Management review provides top management with the opportunity to evaluate the continuing suitability, adequacy, and effectiveness of the QAMS. The management review should cover the scope of the QAMS, although not all elements of the QAMS need to be reviewed at once, and the review process may take place over a period of time. The management review will enable top management to address need for changes to key QAMS elements, including:

a) Policy;
b) Resource allocations;
c) Risk appetite and risk acceptance;
d) Objectives and targets; and
e) Quality assurance strategies.

Review of the implementation and outcomes of the QAMS by top management should be regularly scheduled and evaluated. While ongoing system review is advisable, formal review should be structured, appropriately documented, and scheduled on a suitable basis. Persons who are involved in implementing the QAMS and allocating its resources should be involved in the management review. In addition to the regularly scheduled management system reviews, the following factors can trigger a review and should otherwise be examined once a review is scheduled:

a) *Risk Assessment*: The QAMS should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment can be used to determine whether the QAMS continues to adequately address the risks facing the organization.

b) *Sector/Industry, Contractual, and Political Trends*: Significant changes in sector/industry, contractual, and political trends should initiate a QAMS review. General trends and best practices in the sector/industry and in quality assurance planning techniques can be used for benchmarking purposes.

c) *Regulatory Requirements*: New regulatory requirements may require a review of the QAMS.

d) *Event Experience*: A review should be performed following an undesirable or disruptive event, whether the prevention, mitigation, or response plans were activated or not. If the plans were activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plans were not activated, the review should examine why not, and whether this was an appropriate decision.

e) *Test and Exercise Results*: Based on test and exercise results, the QAMS should be modified as necessary.

Continual improvement and QAMS maintenance should reflect changes in the risks, activities, and operation of the organization that will affect the QAMS. The following are examples of procedures, systems, or processes that may affect the plan:

a) Policy changes;

b) Hazards and threat changes;

c) Changes to the organization and its business processes;

d) Changes in assumptions in risk assessment;

e) Personnel changes (employees and contractors) and their contact information;

f) Subcontractor and supply chain changes;

g) Process and technology changes;

h) Systems and application software changes;

i) Lessons learned from exercising and testing;

j) Lessons learned from external organizations’ undesirable and disruptive events;

k) Issues discovered during actual invocation of the plan;

l) Changes to external environment (new client needs, political changes, relations with local communities, etc.); and

m) Other items noted during review of the plan and identified during the risk assessment.

A.11 Maturity Model for the Phased Implementation

Implementation of a management system standard can be a daunting task, especially for small to medium sized enterprises. All organizations face the challenge of managing their risks within the bounds of organizational objectives and available resources. Only through the full implementation, ongoing maintenance and continual improvement of the QAMS can an organization reach its ultimate goal of assuring quality consistent with respect for human rights. Building the QAMS in a phased approach and achieving benchmarks of maturity, provides the organization a link between objectives and its resources.

By using a maturity model for the phased implementation of the QAMS, the organization defines a series of steps designed to help it evaluate where they currently are with regard to quality assurance and respect for human rights, to set goals for where they want to go, to benchmark where they are relative to those goals, and to plot a business-sensible path to get to full implementation of the QAMS.

Annex B
(informative)

B TERMINOLOGY CONVENTIONS

The terminology conventions in Table 1 are in accordance with ISO/IEC – Directives Part 2: *Rules for the structure and drafting on International Standards, Annex H, Verbal forms for the expression of provisions*, 2004.

Table 1: Verbal forms for the expression of provisions

Verbal form	Usage (ISO/IEC – Directives Part 2: *Rules for the structure and drafting on International Standards*)
shall	Auditable requirements of a document – "used to indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted."
should	Recommendations – "used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited."
may	Permission – "used to indicate a course of action permissible within the limits of the document."
can	Possibility and capability – "used for statements of possibility and capability, whether material, physical or causal."

Items presented in lists should not be construed to be exhaustive, unless otherwise stated. Nor should the order of the list be viewed as specifying a sequence or priority, unless so stated. The generic nature of this *Standard* allows for organization to include additional items, as well as designation of a sequence or priority based on the specific operating conditions and circumstances of the organization.

Annex C
(normative)

C TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in ISO Guide 73:2009, *Risk management- Vocabulary*, and the following apply:

	Term	Definition
C.1	**asset**	Anything that has tangible or intangible value to the organization. Note 1: Tangible assets include human (in this *Standard* considered the most valued), physical, and environmental assets. Note 2: Intangible assets include information, brand, and reputation.
C.2	**audit**	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled Note 1: Internal audits, sometimes called *first party audits*, are conducted by the organization itself, or on its behalf, for management review and other internal purposes (e.g., to confirm the effectiveness of the management system or to obtain information for improvement of the management system). Internal audits may form the basis for an organization's self-declaration of conformity. In many cases, particularly in small organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest. Note 2: External audits include *second* and *third party* audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third party audits are conducted by independent auditing organizations, such as regulators or those providing registration or certification. [ISO 19011:2011]
C.3	**auditor**	Person with the personal attributes and competence to conduct an audit. [ISO 9000:2005]
C.4	**client**	Organization or person that receives a product or service Note 1: Examples include consumers, contractors, end-user, retailer, beneficiary and purchaser. Note 2: A client can be internal (e.g., another division) or external to the organization.

	Term	Definition
C.5	**communication and consultation**	Continual and iterative processes that an organization conducts to provide, share, or obtain information, and to engage in dialogue with stakeholders and others regarding the management of risk. Note 1: The information can relate to the existence, nature, form, likelihood, severity, evaluation, acceptability, treatment, or other aspects of the management of risk and quality assurance management. Note 2: Consultation is a two-way process of informed communication between an organization and its stakeholders or others on an issue prior to making a decision or determining a direction on a particular issue. Consultation is: — A process which impacts on a decision through influence rather than power; and — An input to decision making, not joint decision making. [ISO Guide 73:2009]
C.6	community	A group of associated organizations and groups sharing common interests.
C.7	**competence**	Ability to apply knowledge and skills to achieve intended results .[ISO 19011:2011]
C.8	**conformity**	Fulfillment of a requirement. [ISO 9000:2005]
C.9	**consequence**	Outcome of an event affecting objectives. Note 1: An event can lead to a range of consequences. Note 2: A consequence can be certain or uncertain, and can have positive or negative effects on objectives. Note 3: Consequences can be expressed qualitatively or quantitatively. Note 4: Initial consequences can escalate through knock-on effects. [ISO Guide 73:2009]
C.10	**continual improvement**	Recurring activity to increase the ability to fulfill requirements Note: The process of establishing objectives and finding opportunities for improvement is a continual process through the use of audit findings and audit conclusions, analysis of data, management reviews or other means and generally leads to corrective action or preventive action. [ISO 9000:2005]
C.11	**corrective action**	Action to eliminate the cause of a detected nonconformity or other undesirable situation. Note 1: There can be more than one cause for a nonconformity. Note 2: Corrective action is taken to prevent recurrence, whereas preventive action is taken to prevent occurrence. [ISO 9000:2005]
C.12	**criticality analysis**	A process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a disruption on the organization's ability to meet expectations .
C.13	**critical control point (CCP)**	A point, step, or process at which controls can be applied and a threat or hazard can be prevented, eliminated, or reduced to acceptable levels.

	Term	Definition
C.14	**disruptive event**	An event that interrupts planned activities, operations, or functions, whether anticipated or unanticipated.
C.15	**document**	Information and supporting medium. Note: The medium can be paper, magnetic, electronic, or optical computer disc, photography, or master sample, or a combination thereof. [ISO 9000:2005]
C.16	**effectiveness**	Extent to which planned activities are realized and planned results achieved. [ISO 9000:2005]
C.17	**event**	Occurrence or change of a particular set of circumstances. Note 1: Nature, likelihood, and consequence of an event cannot be fully knowable. Note 2: An event can be one or more occurrences, and can have several causes. Note 3: Likelihood associated with the event can be determined. Note 4: An event can consist of a non-occurrence of one or more circumstances. Note 5: An event with a consequence is sometimes referred to as an *incident*. [ISO Guide 73:2009]
C.18	**exercises**	Evaluating quality assurance management programs, rehearsing the roles of team members and staff, and testing the organization's systems (e.g., technology, reporting protocols, administration) to demonstrate quality assurance management, competence, and capability. Note 1: Exercises include activities performed for the purpose of training and conditioning persons working on behalf of the organization in appropriate responses with the goal of achieving maximum performance.
C.19	**incident**	An event with consequences that has the capacity to cause loss of life, harm to tangible or intangible assets, or negatively impact human rights and fundamental freedoms of internal or external stakeholders.
C.20	**integrity**	The property of safeguarding the accuracy and completeness of assets. [ISO/IEC 13335-1:2004]
C.21	**likelihood**	Chance of something happening. Note: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). [ISO Guide 73:2009]
C.22	**management plan**	Clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the event management process.

	Term	Definition
C.23	**management system**	System to establish policy and objectives and to achieve those objectives. Note: Management systems are used by organizations to develop their policies and to put these into effect via objectives and targets, using: — An organizational structure where the roles, responsibilities, authorities, etc., of people are defined; — Systematic processes and associated resources to achieve the objectives and targets: — Measurement and evaluation methodology to assess performance against the objectives and targets, with feedback of results used to plan improvements to the system; and — A review process to ensure problems are corrected and opportunities for improvement are recognized and implemented, when justified. [ISO Guide 72:2001]
C.24	**monitoring**	Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected. [ISO Guide 73:2009]
C.25	**nonconformity**	Non-fulfillment of a requirement. [ISO 9000:2005]
C.26	**norms**	Recognized and accepted rules of social behavior.
C.27	**organization**	Group of people and facilities with an arrangement of responsibilities, authorities, and relationships. Note: An organization can be a government or public entity, company, corporation, firm, enterprise, institution, charity, sole trade or association, or parts or combinations thereof.
C.28	**planning**	Part of management focused on setting quality assurance objectives and specifying necessary operational processes and related resources to fulfill the quality assurance objectives.
C.29	**prevention**	Measures that enable an organization to avoid, preclude, or limit the impact of an undesired or potentially disruptive event.
C.30	**preventive action**	Action to eliminate the cause of a potential nonconformity or other undesirable potential situation. Note 1: There can be more than one cause for a potential nonconformity. Note 2: Preventive action is taken to prevent occurrence, whereas corrective action is taken to prevent recurrence. [ISO 9000:2005]

	Term	Definition
C.31	**private security companies** and **private security service providers (collectively known as PSCs)**	Any organization whose business activities include the provision of security services either on its own behalf or on behalf of another. Note 1: PSCs provide services to clients with the aim of ensuring their security and that of others. Note 2: PSCs typically work in high risk environments and provide services for which personnel are required to carry weapons in the performance of their duties in accordance with the terms of their contract. Note 3: Example of security services provided by PSCs may include: guarding; close protection; physical protection measures; security awareness; risk, security, and threat assessment; the provision of protective and defensive measures for compounds, diplomatic, and residential perimeters; escort of transport; and policy analysis.
C.32	**procedure**	Specified way to carry out an activity or a process. Note 1: Procedures can be documented or not. Note 2: When a procedure is documented, the terms *written procedure* or *documented procedure* are frequently used. The document that contains a procedure can be called a *procedure document*. [ISO 9000:2005]
C.33	**quality assurance management**	Coordinated activities to direct and control an organization with regard to quality assurance. Note: Direction and control with regard to quality assurance management generally includes establishment of the policy, planning, and objectives directing operational processes and continual improvement.
C.34	**quality assurance objective**	Something sought, or aimed for, related to quality assurance. Note 1: Quality objectives are generally based on the organization's quality policy. Note 2: Quality objectives are generally specified for relevant functions and levels in the organization.
C.35	**quality assurance policy**	Overall intentions and direction of an organization related to quality assurance as formally expressed by top management. Note 1: Generally, the quality assurance policy is consistent with the overall policy of the organization, and provides a framework for the setting of quality assurance objectives. Note 2: Quality assurance management principles presented in this *Standard* can form a basis for the establishment of a quality policy consistent with the principles and obligations outlined in the ICoC and *Montreux Document*.
C.36	**record**	Document stating results achieved or providing evidence of activities performed. Note: Records can be used, for example, to document traceability and to provide evidence of verification, preventive action, and corrective action. [ISO 9000:2005]

	Term	Definition
C.37	**residual risk**	Risk remaining after risk treatment. Note 1: Residual risk can contain unidentified risk. Note 2: Residual risk can also be known as *retained risk*. [ISO Guide 73:2009]
C.38	**resilience**	Adaptive capacity of an organization in a complex and changing environment. [ISO Guide 73:2009]
C.39	**resources**	Any asset (human, physical, information, or intangible), facilities, equipment, materials, products, or waste that has potential value and can be used. [ANSI/ASIS.SPC.1:2009]
C.40	**review**	Activity undertaken to determine the suitability, adequacy, and effectiveness of the management system and its component elements to achieve established objectives.
C.41	**risk**	Effect of uncertainty on objectives. Note 1: An *effect* is a deviation from the expected — positive and/or negative. Note 2: Objectives can have different aspects (such as protection of human rights, legal compliance, financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process). Note 3: Risk is often characterized by reference to potential events and consequences, or a combination of these. Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. [ISO Guide 73:2009]
C.42	**risk acceptance**	Informed decision to take a particular risk. Note 1: Risk acceptance can occur without risk treatment or during the process of risk treatment. Note 2: Accepted risks are subject to monitoring and review. [ISO Guide 73:2009]
C.43	**risk analysis**	Process to comprehend the nature of risk and to determine the level of risk. Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2: Risk analysis includes risk estimation. [ISO Guide 73:2009]
C.44	**risk appetite**	Amount and type of risk that an organization is prepared to pursue, retain or take. [ISO Guide 73:2009]
C.45	**risk assessment**	Overall process of risk identification, risk analysis, and risk evaluation. [ISO Guide 73:2009]

	Term	Definition
C.46	**risk criteria**	Terms of reference against which the significance of a risk is evaluated. Note 1: Risk criteria are based on organizational objectives, and external and internal context. Note 2: Risk criteria can be derived from standards, laws, policies, and other requirements. [ISO Guide 73:2009]
C.47	**risk evaluation**	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Note: Risk evaluation assists in the decision about risk treatment. [ISO Guide 73:2009]
C.48	**risk identification**	Process of finding, recognizing, and describing risks. Note 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs. [ISO Guide 73:2009]
C.49	**risk management**	Coordinated activities to direct and control an organization with regard to risk. [ISO Guide 73:2009]
C.50	**risk register**	A compilation for all risks identified, analyzed, and evaluated in the risk assessment process. Note: The risk register includes information on likelihood, consequences, treatments, and risk owners.
C.51	**risk tolerance**	Organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Note: Risk tolerance can be influenced by client, stakeholder, legal, or regulatory requirements. [ISO Guide 73:2009]

	Term	Definition
C.52	**risk treatment**	Process to modify risk. Note 1: Risk treatment can involve: — Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — Taking or increasing risk in order to pursue an opportunity; — Removing the risk source; — Changing the likelihood; — Changing the consequences; — Sharing the risk with another party or parties (including contracts and risk financing); and — Retaining the risk by informed choice. Note 2: Risk treatments that deal with negative consequences are sometimes referred to as *risk mitigation*, *risk elimination*, *risk prevention*, and *risk reduction*. Note 3: Risk treatment can create new risks or modify existing risks. [ISO Guide 73:2009]
C.53	**security**	The condition of being protected against hazards, threats, risks, or loss. Note 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside. Note 2: The term *security* means that something not only is secure, but that it has been secured. [ANSI/ASIS.SPC.1:2009]
C.54	**self-defense**	The use of reasonable force in defense of oneself or others. Note 1: Deadly force should only be used in self-defense or the defense of others, when it reasonably appears necessary to prevent the commission of a serious offense involving violence threatening death or serious bodily harm.
C.55	**stakeholder**	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. Note: A decision maker can be a stakeholder. [ISO Guide 73:2009]
C.56	**supply chain**	The linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user. Note: The supply chain may include vendors, subcontractors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user.
C.57	**target**	Detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives. [ISO 14001:2004]
C.58	**threat analysis**	Process of identifying and quantifying the potential cause of an unwanted event, which may result in harm to individuals, assets, a system or organization, the environment, or the community.

	Term	Definition
C.59	**top management**	Person or group of people who directs and controls an organization at the highest level. [ISO 9000:2005]
C.60	**undesirable event**	Any event that has the potential to cause loss of life, harm to tangible or intangible assets, or negatively impact human rights and fundamental freedoms of internal or external stakeholders.
C.61	**use of force continuum**	The force applied may be increased or decreased as a continuum relative to the response of the adversary, using the amount of force required to compel compliance. Note 1: The amount of force used should be the minimum amount needed to eliminate the threat presented, thereby minimizing the risk and severity of any injury that may occur. Note 2: Escalation/de-escalation of force response with a level of force should be appropriate to the situation at hand, acknowledging that the response may move from one part of the continuum to another in a matter of seconds.
C.62	**vulnerability analysis**	Process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence.
C.63	**worst forms of child labor**	The worst forms of child labor comprises: a) All forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom, and forced or compulsory labor, including forced or compulsory recruitment of children for use in armed conflict. b) The use, procuring, or offering of a child for prostitution; for the production of pornography; or for pornographic performances. c) The use, procuring, or offering of a child for illicit activities, in particular for the production and trafficking of drugs as defined in the relevant international treaties. d) Work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children. [C182 Worst Forms of Child Labour Convention, 1999, Article 3. < http://www.ilo.org/ilolex/cgi-lex/convde.pl?C182 >]

Annex D
(informative)

D QUALIFIERS TO APPLICATION

The adoption and implementation of a range of quality assurance management techniques in a systematic manner can contribute to optimal outcomes for all stakeholders and affected parties. However, adoption of this *Standard* will not by itself guarantee optimal quality assurance outcomes. In order to achieve its objectives, the QAMS should incorporate the best available practices, techniques, and technologies, where appropriate and where economically viable. The cost-effectiveness of such practices, techniques, and technologies should be taken fully into account.

This *Standard* does not establish absolute requirements for quality assurance performance beyond commitments in the organization's policy to:

a) Comply with applicable legal requirements and with other requirements to which the organization subscribes;

b) Support prevention of undesirable and disruptive events and risk minimization; and

c) Promote continual improvement.

The main body of this *Standard* contains only those generic criteria that may be objectively audited. Guidance on supporting quality assurance management techniques is contained in the other annexes of this document.

This *Standard*, like other management standards, is not intended to be used to create non-tariff trade barriers or to increase or change an organization's legal obligations. Indeed, compliance with a standard does not in itself confer immunity from legal obligations. For organizations that so wish, an external or internal auditing process may verify compliance of their QAMS to this *Standard*. Verification may be by an acceptable first-, second-, or third-party mechanism. Verification does not require third-party certification.

This *Standard* does not include requirements specific to other management systems, such as those for quality, occupational health and safety, or resilience management – though its elements can be aligned or integrated with those of other management systems. It is possible for an organization to adapt its existing management system(s) in order to establish a QAMS that conforms to the criteria of this *Standard*. It should be understood, however, that the application of various elements of the management system might differ depending on the intended purpose and the stakeholders involved.

The level of detail and complexity of the QAMS, the extent of documentation, and the resources devoted to it will be dependent on a number of factors – such as the scope of the system; the size of an organization; and the nature of its activities, products, services, and supply chain. This may be the case in particular for small and medium-sized enterprises.

This *Standard* provides a common set of criteria for quality assurance management programs. Terminology used in this *Standard* emphasizes commonality of concepts, while acknowledging nuances in term usage in the various disciplines. For consistency with ISO 31000:2009, risk assessment is the process of risk identification, analysis, and evaluation.

Annex E
(informative)

E BIBLIOGRAPHY

E.1 References

International Code of Conduct for Private Security Service Providers (ICoC) of 9 November 2010. [Online]. Available: < http://www.icoc-sp.org/uploads/INTERNATIONAL_CODE_OF_CONDUCT_Final_without_Company_Names.pdf > Accessed 2011, September 8.

Swiss Confederation, Federal Department of Foreign Affairs (2008) *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 [Online]. Available: < http://www.un.org/ga/search/view_doc.asp?symbol=A/63/467 > Accessed 2011, September 8.

E.2 ASIS International Publications[3]

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

E.3 National Standards Publications[3]

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

ASIS International (2012), ANSI/ASIS SPC.4-2012, *Maturity Model for the Phased Implementation of the Organizational Resilience Management System.*

E.4 ISO Standards Publications[4]

ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*.

ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*.

ISO 19011:2011, *Guidelines for quality and/or environmental management systems auditing*.

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

[3] These documents are available at < http://www.asisonline.org >.

[4] These documents are available at < http://www.iso.org >.

ISO Guide 72:2001, *Guidelines for the justification and development of management system standards.*

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

ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1.*

ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*.

E.5 United Nations and International Human Rights Publications

Convention Relative to the Protection of Civilian Persons in Time of War (Geneva Convention IV), August 12, 1949; < http://www.icrc.org/ihl.nsf/INTRO/380 >, accessed 2 March 2012.

Convention Respecting the Laws and Customs of War on Land (Hague IV); October 18, 1907; < http://avalon.law.yale.edu/20th_century/hague04.asp >, accessed 2 March 2012.

International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva, © ICRC, May 2009.

Parks, W. Hays, *Evolution of Policy and Law Concerning the Role of Civilians and Civilian Contractors Accompanying the Armed Forces*, Washington, DC, (c) 2005, W. Hays Parks.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, < http://www.icrc.org/ihl.nsf/INTRO/475?OpenDocument >, accessed 2 March 2012.

United Nations, *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*, 1990, < http://www2.ohchr.org/english/law/firearms.htm >.

United Nations. *The Convention against Torture and Other Cruel, Inhuman or Other Degrading Treatment of Punishment* (CAT) 1984. < http://www2.ohchr.org >

United Nations. *The Convention of the Elimination of All Forms of Discrimination against Women* (CEDAW) 1979. < http://www.un.org >

United Nations. *The Convention on the Prevention and Punishment of the Crime of Genocide* 1948; < http://www.un.org >

United Nations. *The Convention on the Rights of the Child* (CRC) 1989. < http://www2.ohchr.org >

United Nations. *Global Compact Principles*. Retrieved December 20, 2011. < http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html >

United Nations. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN A/HRC/17/31 21 March 2011. < http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf >

United Nations. *ILO Declaration on Fundamental Principles and Rights at Work.* International Labour Conference, Eighty-sixth Session, Geneva, 18 June 1998 (Annex revised 15 June 2010) < http://www.ilo.org/declaration/thedeclaration/textdeclaration/lang--en/index.htm >

United Nations. *The International Covenant on Civil and Political Rights* (ICCPR) 1966. < http://www2.ohchr.org >

United Nations. *The International Covenant on Economic, Social and Cultural Rights* (ICESCR) 1966. < http://www2.ohchr.org >

United Nations. *The International Convention on the Elimination of All Forms of Racial Discrimination* (ICERD) 1966. < http://www2.ohchr.org >

United Nations. *The Universal Declaration of Human Rights* 1948; < http://www.un.org >

United Nations. *Protect, Respect, and Remedy: a Framework for Business and Human Rights* UN A/HRC/8/5 7 April 2008.
< http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf >

U.S. Department of Defense, Department of Defense Directive 5210.56, *Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities*, Washington DC, USGPO, 1 April 2011

Voluntary Principles on Security and Human Rights. Retrieved December 20, 2011.
< http://www.voluntaryprinciples.org/files/voluntary_principles_english.pdf > Maintained by Foley Hoag LLP, the Secretariat for the Voluntary Principles on Security and Human Rights

ASIS
INTERNATIONAL
Advancing Security Worldwide®

ASIS International (ASIS) is the preeminent organization for security professionals, with 38,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the general public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management*, ASIS leads the way for advanced and improved security performance. For more information, visit *www.asisonline.org.*

ASIS
INTERNATIONAL
Advancing Security Worldwide®

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

ISBN 978-1-934904-33-6
9 781934 904336