ASIS
INTERNATIONAL
Advancing Security Worldwide®

STANDARD

Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations

ASIS PSC.2-2019

Abstract

This Standard provides requirements and guidance for conducting conformity assessment of the ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations – Requirements with Guidance Standard. It provides requirements for bodies providing auditing and third party certification of Private Security Company Operations (PSCs) – private security providers working for any client in conditions where governance and the rule of law have been undermined by conflict or disaster.

The worldwide leader in security standards and guidelines development

ANSI/ASIS PSC.2-2019 (revision of 2012)

Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations

Approved 23 May 2019

ASIS International

Abstract

This *Standard* provides requirements and guidance for conducting conformity assessment of the ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations – Requirements with Guidance Standard. It provides requirements for bodies providing auditing and third party certification of Private Security Company Operations (PSCs) – private security providers working for any client in conditions where governance and the rule of law have been undermined by conflict or disaster. It provides requirements and guidance on the management of audit programs, conduct of internal or external audits of the management system and private security company operations, as well as on competence and evaluation of auditors.

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's or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify, or reject. Any certification or other statement of compliance with any information in this document should not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the *Standard.*

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

About ASIS

Founded in 1955, ASIS International is the world's largest membership organization for security professionals. With hundreds of chapters across the globe, ASIS is recognized as the premier source for learning, networking, standards, and research. Through its board certifications, award-winning *Security Management* magazine, and the Global Security Exchange—the most influential event in the profession—ASIS ensures its members and the security community have access to the intelligence and resources necessary to protect their people, property, and information assets. Learn more about the work we do at asisonline.org.

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 (ISO). 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.

ASIS COMMISSION ON STANDARDS AND GUIDELINES

Chairman: Bernard Greenawalt, CPP, Securitas Security Services USA (retired)
Vice-chair: Werner Cooreman, CPP, PSP, Solvay

Charles Baley, Farmers Group, Inc.
Bruce Braes, CPP, Jacobs UK Ltd.
Robert Carotenuto, CPP, PCI, PSP, The New York Botanical Garden
Michael Crane, CPP, Securisks
David Dodge, CPP, PCI, David Dodge & Associates
Lisa DuBrock, CPP, Radian Compliance
Linda Florence, CPP, The Florence Group
Tommy Hansen, CPP, Petroleum Safety Authority
Ronald Lander, CPP, Ultrasafe Security Solutions
Bryan Leadbetter, CPP, Arconic
Ronald Martin, CPP, Open Security Exchange
Juan Muñoz, CPP, Associated Projects International
Angela Osborne, PCI, Guidepost Solutions
Werner Preining, CPP, Interpool Security
Malcolm Reid, CPP, Brison
Jeffrey Slotnick, CPP, PSP, Setracon Enterprise Security Risk Management Services
J. Kelly Stewart, Newcastle Consulting, LLC
Timothy Sutton, CPP, Guidepost Solutions
John Villines, CPP, PCI, PSP, John C. Villines LLC
Roger Warwick, CPP, Pyramid Temi Group
Allan Wick, CPP, PCI, PSP, Tri-State Generation & Transmission

At the time it approved this document, the PSC.2 Committee, which is responsible for the revision of this *Standard*, had the following members:

COMMITTEE MEMBERS

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

Commission Liaison: Lisa DuBrock, Radian Compliance

Committee Secretariat: Aivelis Opicka, ASIS International

Mark Beaudry, CPP, IBM
James Cameron, CPP, Security Concepts Group
Antony Chattin, MSS Global Ltd
David Dodge, CPP, PCI, David Dodge & Associates
Jack Dowling, CPP, PSP, J D Security Consultants
Michael Edgerton, CPP, HudsonTrident
James Ellis, CPP, PSP, Principal Financial Group
Mark Folmer, CPP, TrackTik
Richard Hough, University of West Florida
Michael Kaufman, St. Louis County Police
    Department
Anaïs Laigle, ICoCA
Natalia Larrimer, ANAB

Tanya Leakey, KK Security
Sorcha MacLeod, Free University Berlin and Berlin
    School of Law and Economics
John Maina, KK Security
Ronald Martin, CPP, Open Security Exchange
Christopher Mayer, U.S. Department of Defense
Oona Muirhead, MSS Global Ltd
Karel Simpson, GardaWorld International Protective
    Service
Jeffrey Slotnick, CPP, PSP, Setracon Enterprise
    Security Risk Management Services
Jamie Williamson, ICoCA

WORKING GROUP MEMBERS

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

Mark Beaudry, CPP, IBM
James Cameron, CPP, Security Concepts Group
Antony Chattin, MSS Global Ltd
David Dodge, CPP, PCI, David Dodge & Associates
Michael Edgerton, CPP, HudsonTrident
James Ellis, CPP, PSP, Principal Financial Group
Mark Folmer, CPP, TrackTik
Richard Hough, University of West Florida
Michael Kaufman, St. Louis County Police
    Department

Anaïs Laigle, ICoCA
Natalia Larrimer, ANAB
Sorcha MacLeod, Free University Berlin and Berlin
    School of Law and Economics
John Maina, KK Security
Christopher Mayer, U.S. Department of Defense
Karel Simpson, GardaWorld International Protective
    Service
Jeffrey Slotnick, CPP, PSP, Setracon Enterprise
    Security Risk Management Services

TABLE OF CONTENTS

INTRODUCTION

General

Conformity assessment and certification of the Quality Assurance Management System (QAMS)[1] of an organization is one means of providing assurance that any type of private security service provider has implemented a system for the management of quality of service in line with its policy and consistent with respect for human rights, legal obligations, and good practices, as specified in the ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations – Requirements with Guidance.

This *Standard* is a sector-specific standard based on the ISO/IEC 17021-1:2015 and provides additional requirements for conformity assessment in those areas that are deemed necessary and relate specifically to any type of Private Security Service Providers, including Private Security Companies (collectively "PSCs"), operating in circumstances of weakened governance or 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 ongoing, 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.

This *Standard* has been developed to assist in the certification of quality assurance management systems that fulfill the requirements of ANSI/ASIS PSC.1-2012 (R2017). The contents of this *Standard* may also be used to support certification of quality assurance management systems that are based on other or additional sets of specified requirements.

This *Standard* is intended for use by bodies that carry out audit, conformity assessment, and certification of quality assurance management systems. It gives generic requirements for certification bodies that perform audit, conformity assessment, and certification of PSCs' management systems. Such bodies are referred to as "certification bodies." This *Standard* is also usable by anybody involved in the conformity assessment of quality assurance management systems.

Certification activities involve the audit of an organization's QAMS. The form of attestation of conformity of an organization's QAMS to the QAMS standard or other specified requirements is normally a certification document or a certificate.

The organization being certified develops its own management systems tailored to its needs and resources and, except where relevant legal requirements specify to the contrary, it is for the organization to decide how the various components of the management system will be arranged. The degree of integration between various management system components will vary from organization to organization. It is therefore appropriate for certification bodies that operate in accordance with this *Standard* to take into account the culture and practices of their clients with respect to the integration of their quality assurance management systems within the wider organization.

---

[1] For Private Security Service Providers seeking conformity assessment and certification to ISO 18788:2015, the ANSI/ASIS PSC.2-2019 can be used as guidance. In the ISO 18788:2015, QAMS is referred to as the Security Operations Management System (SOMS).

Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations

1. SCOPE

This *Standard*:

a) Is a sector-specific standard based on the ISO/IEC 17021-1:2015;

b) Describes the process that needs to be followed to conduct attestation of fulfillment of the requirements of the standard ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations – Requirements with Guidance;

c) Provides requirements and guidance for conducting conformity assessment of the ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations – Requirements with Guidance Standard;

d) Provides requirements for bodies providing auditing and third party certification of PSCs working for any client (public, private, non-governmental, or not-for-profit);

e) Provides requirements and guidance on the management of audit programs and the conduct of internal or external audits of the management system and PSC operations, as well as on competence and evaluation of auditors; and

f) Provides confidence and information to internal and external stakeholders that the requirements of the ANSI/ASIS PSC.1-2012 (R2017) are being met.

Conformity assessment is the process used to demonstrate that a product, service, management system, or body meets specified criteria and requirements; in the case of this *Standard*, the criteria and requirements of the ANSI/ASIS PSC.1-2012 (R2017). There are three types of conformity assessment:

a) First party - Carried out by the organization itself or by someone working on behalf of the organization. It is a self-assessment and self-declaration.

b) Second party - Performed by a client or customer of the organization.

c) Third party - Performed by a body that is independent of the organization that provides the product/services and is not a user of the product/services. An independent certification body certifies that another organization complies with the standard and issues it with a certificate to this effect.

Certification of a quality assurance management system ("certification") is a third party conformity assessment activity. Bodies performing this activity are therefore third party conformity assessment bodies ("certification body").

NOTE 1: Certification of a management system is sometimes also called "registration" and certification bodies are sometimes called "registrars."

NOTE 2: A certification body can be non-governmental or governmental (with or without regulatory authority).

NOTE 3: This *Standard* is primarily intended to be used as a criteria document for the accreditation or peer assessment of certification bodies which seek to be recognized as being competent to certify that a quality assurance management system complies with ANSI/ASIS PSC.1-2012 (R2017). It is also intended to be used as a criteria document by regulatory authorities and

clients of PSCs which engage in direct recognition of certification bodies to certify that a quality assurance management system complies with ANSI/ASIS PSC.1-2012 (R2017). The *Standard*'s requirements may also be useful to any other parties involved in the conformity assessment of such certification bodies.

Organizations can use the concepts and requirements of this *Standard* for first and second party conformity assessment provided that the requirements are adapted as necessary. It is recommended that organizations implementing the ANSI/ASIS PSC.1-2012 (R2017) use the procedures described in this *Standard* in conjunction with the ISO 19011:2018 to conduct their internal audit activities.

2. NORMATIVE REFERENCES

The following documents contain information which, through reference in this text, are indispensable for the application 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) ISO 9000:2015, Quality management systems — Fundamentals and vocabulary.[2]

b) ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles.[2]

c) ISO/IEC 17021-1:2015, Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements.[2]

d) ISO 19011:2018, Guidelines for auditing management systems.[2]

e) ANSI/ASIS PSC.1-2012 (R2017), Management System for Quality of Private Security Company Operations - Requirements with Guidance.[3]

f) International Code of Conduct (ICoC) for Private Security Service Providers (11/2010).[4]

g) 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).[5]

3. TERMS AND DEFINITIONS

For the purposes of this *Standard* the terms and definitions in ISO 9000; ISO/IEC 17000; ISO/IEC 17021-1; ISO 19011; and ANSI/ASIS PSC.1 apply.

4 PRINCIPLES

All the principles of auditing and certification from ISO/IEC 17021-1:2015 apply. In addition, the following PSC-specific guidance principles apply.

4.1 General

The principles in this *Standard* give guidance necessary to provide transparency, confidence, and trust in the auditing, conformance assessment, and certification processes. Conformity assessment provides confidence to

---

[2] This document is available at < http://www.iso.org >.

[3] This document is available at < http://www.asisonline.org>. The ISO equivalent of ANSI/ASIS PSC.1-2012 (R2017) is the ISO 18788:2015.

[4] This document is available at < http://icoca.ch/en/the_icoc>.

[5] This document is available at < http://www.un.org/ga/search/view_doc.asp?symbol=A/63/467 >.

internal and external stakeholders that the requirements of the ANSI/ASIS PSC.1-2012 (R2017) standard are being met. Stakeholders that have an interest in attestation to conformance include, but are not limited to:

a) PSCs;

b) Current and prospective clients of the PSCs;

c) Supply chain partners, subcontractors, and insurance providers;

d) Local and affected communities;

e) International, non-governmental, and human rights organizations; and

f) Local, national, and international government authorities and bodies.

4.2   Impartiality

Confidence in the auditing and conformity assessment process is dependent on an independent and impartial evaluation of the management system. Impartiality requires both the actual and perceived presence of objectivity. Certification bodies need to implement measures to assure and monitor impartiality to demonstrate to internal and external stakeholders that there is a credible auditing and conformity assessment process.

4.3   Competence

Competence is the ability to apply knowledge and skills to achieve intended results. Competence of the personnel of the certification body in all functions involved in certification activities in the fields of risk management, security functions, quality assurance, and principles of law directly associated with the preservation or promotion of human rights is necessary to deliver certification that provides confidence.

4.4   Responsibility

Conformance to the requirements of the ANSI/ASIS PSC.1-2012 (R2017) standard is the responsibility of the PSC organization implementing the standard. It is the responsibility of the auditing team and certification body to objectively evaluate conformance to the criteria of the ANSI/ASIS PSC.1-2012 (R2017) standard by collecting and documenting evidence of conformance or non-conformance to the ANSI/ASIS PSC.1-2012 (R2017) standard's requirements. Sufficient documented evidence is necessary for a declaration of conformance.

4.5   Openness and Transparency

The certification body needs to provide appropriate access to, or disclosure of, non-confidential information about the conclusions of specific audits (e.g. validation of certification status) to specific documented interested parties. Given the nature of operations and environment in which PSCs operate, care must be taken to protect the security, rights, and privacy of internal and external stakeholders, as well as inform the PSC of any information provided to stakeholders.

4.6   Confidentiality

To gain the privileged access to information that is needed for the auditing and conformity assessment process, the certification body needs to keep confidential any sensitive, proprietary, and/or risk-related information about an organization and its management system, as well as information that may cause harm to the PSCs' clients, persons who work on their behalf, complainants, and other external stakeholders.

4.7   Responsiveness to Complaints

Parties that rely on certification expect to have complaints documented and investigated in a fair and impartial process. Appropriate corrective and preventive actions should be taken expeditiously to remedy the situation and prevent a recurrence. The certification body should have a documented policy for receiving, processing, investigating, and responding to complaints including a defined timeline for resolution. Affected parties should be informed of the outcomes of the complaints process to maintain credibility of the auditing and conformity assessment process. An appropriate balance between the principles of openness and confidentiality, including responsiveness to complaints, is necessary in order to demonstrate integrity and credibility to all users of certification.

4.8   Vetting of Auditors

The credibility of any auditing and conformity assessment process is a function of the competence and reputation of the auditors. All auditors should be vetted to assure an appropriate level of:

a)   Technical competence;

b)   Understanding of the operational environment of PSCs;

c)   Respect for human rights;

d)   Ethical behavior;

e)   Impartiality; and

f)   Background screening and relevant security clearances.

4.9   Risk-based Approach

Certification bodies need to take into account the risks associated with providing competent, consistent, and impartial certification. Risks may include, but are not limited to, those associated with:

a)   The objectives of the audit;

b)   The sampling used in the audit process;

c)   Real and perceived impartiality;

d)   Legal, regulatory, and liability issues;

e)   The client organization being audited and its operating environment;

f)   Impact of the audit on the client and its activities;

g)   Health and safety of the audit teams;

h)   Perception of interested parties;

i)   Misleading statements by the certified client; and

j)   Use of marks.

5.   GENERAL REQUIREMENTS

All the requirements from ISO/IEC 17021-1:2015, section 5, apply. In addition, the following PSC-specific requirements apply.

5.1   Legal and Contractual Matters

The certification body shall have a legally enforceable agreement for the provision of certification activities to its client. Where there are multiple sites of a certified client, the certification body shall ensure there is a legally enforceable agreement between the certification body granting certification explicitly covering each certified site of the client. The agreement shall clearly define the scope of the certification and to which standard(s) and/or other normative documents the certification shall take place.

5.2   Management of Impartiality

The certification body, and any part of the same legal entity, shall not offer or provide human rights impact assessment consultancy, QAMS consultancy or management system consultancy, or internal audit services to clients being audited.

The fact that the organization employing the auditor is known to have provided consultancy or internal audit services within two years of an audit is considered as a significant threat to impartiality. Therefore, the certification body shall not certify a management system on which it provided consultancy or internal audit services within two years following the end of the internal audits.

5.3   Liability and Financing

All the requirements from ISO/IEC 17021-1:2015, section 5.3, apply.

6.   STRUCTURAL REQUIREMENTS

All the requirements from ISO/IEC 17021-1:2015, section 6, apply. In addition, the following PSC-specific requirements apply.

6.1   Organizational Structure and Top Management

The certification body shall have a documented organizational structure to give accountability and provide confidence in its certification.

6.2   Committee for Safeguarding Impartiality

The certification body shall establish a committee to safeguard the impartiality of its activities. The committee shall be comprised of a balance of interests, recognizing that this committee cannot represent every interest. The certification body should identify and invite key interest parties, such as:

a)   Clients of the certification body;

b)   Customers of organizations whose quality assurance management systems are certified;

c)   Representatives of industry trade associations;

d)   Representatives of PSC client organizations;

e)   Representatives of governmental bodies; and

f)   Representatives of non-governmental human rights and international humanitarian law (IHL) organizations and other directly affected stakeholders.

7. RESOURCE REQUIREMENTS

All the requirements from ISO/IEC 17021-1:2015, section 7, apply. In addition, the following PSC-specific requirements apply.

7.1 Competence of Management and Personnel

All the requirements from ISO/IEC 17021-1:2015, section 7.1, apply. In addition, the following PSC-specific requirements apply.

7.1.1 General Considerations

The certification body shall determine and document the competence required to evaluate each PSC technical area and function in the certification activity. When identifying competence requirements, the certification body shall tailor its competence requirements to the types of services the PSC provides and the theater of operations in order to:

a) Define the scope of the activities that it undertakes;

b) Identify any technical qualification of its auditors necessary for that particular type of service and theater of operation;

c) Ensure that personnel have appropriate knowledge, skills, and experience relevant to types of services provided and geographic areas of operation; and

d) Select a suitably qualified audit team.

The certification body shall determine the means for the demonstration of competence prior to carrying out specific functions. Records of the determination shall be maintained.

7.1.2 Determination of Competence Criteria

The certification body shall have a documented process for determining the competence criteria for personnel with a demonstrated capacity for the management and performance of audits and certification. Measurable criteria shall be determined to demonstrate competence with regards to:

a) The requirements of ANSI/ASIS PSC.1-2012 (R2017) quality assurance management system standard;

b) Quality, security, and risk assessment and management 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;

c) The legal, cultural, and operational context of the theater of operation; and

d) Functions in the certification process.

The output of the process shall be the documented criteria of required knowledge and skills necessary to effectively perform audit and certification tasks to be fulfilled to achieve the intended results.

7.2 Personnel Involved in the Certification Activities

All the requirements from ISO/IEC 17021-1:2015, section 7.2, apply. In addition, the following PSC-specific requirements apply.

The certification body shall ensure that all persons working on its behalf assigned to perform quality assurance certification audits—as well as technical experts—as far as these have contact with confidential information, can be trusted to maintain confidential information obtained during auditing and conformity assessment work and that they do not create a security risk such as betraying confidentiality or adversely impacting operations.

All persons working on behalf of the certification body assigned to perform quality assurance management system audits shall have as a minimum personal attributes, knowledge, and skills as described in ISO/IEC 17021-1:2015, Annexes A and D, relevant to quality assurance management.

7.3 Competences Required for Auditing and Conformity Assessment of Quality Assurance Management Systems

7.3.1 Generic Knowledge and Skills of Management System Auditors

All persons working on behalf of the certification body assigned to perform quality assurance management system audits and conformity assessment shall have as a minimum the generic knowledge and skills of management system auditors as described in ISO/IEC 17021-1:2015.

7.3.2 Management System Knowledge and Skills

Knowledge and skills in this area shall cover:

a) Management system principles and the application of management systems to different organizations;

b) The interaction between the components of the management system;

c) The ANSI/ASIS PSC.1-2012 (R2017) quality assurance management system standard, applicable procedures, or other documents (ICoC and *Montreux Document*), used as audit criteria;

d) Recognizing the hierarchy of reference documents;

e) Application of the reference documents to different audit situations; and

f) Information control processes for authorization, security, distribution, and control of documents, data, and records.

7.3.3 Organizational Context Knowledge and Skills

All persons working on behalf of the certification body assigned to perform QAMS audits and conformity assessment shall have as a minimum the organizational context knowledge and skills of management system auditors as described in ISO/IEC 17021-1:2015.

7.3.4 Applicable Laws, Regulations, and Other Requirements Relevant to the Discipline

All persons working on behalf of the certification body assigned to perform QAMS audits and conformity assessment shall have the knowledge and skills necessary to work within, and be aware of, the requirements that apply to the organization being audited. Knowledge and skills in this area shall cover:

a) IHL, legal obligations under human rights law, and other relevant international law;

b) Legal obligations and good practices described in the *Montreux Document* and foundational principles in the ICoC;

c) Local, regional, and national codes, laws and regulations;

d) Contracts and agreements; and

e) Other requirements to which the organization subscribes.

7.3.5 Discipline-specific Knowledge and Skills of Auditors in Quality Assurance of PSCs

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes, and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions. Persons conducting QAMS auditing and conformity assessment shall

have competencies in assessing and managing the risks related to PSCs' services, functions, and environment in which they operate. This includes but is not limited to:

a) Understanding the requirements of the ANSI/ASIS PSC.1-2012 (R2017) quality assurance management system standard;

b) Understanding the roles and responsibilities of PSC clients, government, and subcontractors;

c) Managing the risks of undesirable and disruptive events (assess, anticipate, avoid, prevent, protect, mitigate, respond to, and recover);

d) Knowledge of human rights and IHL, and the role of human rights and IHL non-governmental organizations;

e) Terminology, processes, science, and technology relevant to the PSC sector;

f) Terminology, practice, and understanding of the rule of law and use of force, including those concerning weapons training and handling, security measures, personnel protection, and apprehension of persons;

g) Measures for personal safety and security in theaters of operation;

h) Methods for information gathering and monitoring;

i) Human rights impact assessment and risks related to protection of human rights;

j) Risk assessment (asset identification and valuation, as well as risk identification, analysis, evaluation) related to tangible and intangible assets;

k) Risk treatment (minimize likelihood and mitigate consequences);

l) Knowledge of incident communications and reporting protocols;

m) Methods and practices for information integrity and sensitivity;

n) Methods for personnel security and protection of persons;

o) Methods and practices for asset protection and physical security;

p) Methods and practices for avoidance, prevention, and deterrence management;

q) Methods and practices for incident mitigation, preparedness, response, and crisis management;

r) Methods and practices for continuity, emergency, and recovery management; and

s) Methods and practices for monitoring, measuring, and reporting of performance (including exercise and testing methodologies).

7.3.6   Training and Experience

Persons conducting QAMS auditing and conformity assessment shall have successfully completed training and be able to demonstrate competence in the understanding and application of:

a) Management systems auditing;

b) Quality assurance management methodologies;

c) Risk assessment and management principles;

d) IHL, legal obligations under human rights law, and other relevant international law;

e) Legal obligations and good practices described in the *Montreux Document* and foundational principles in the ICoC; and

f) Managing the risks of undesirable and disruptive events.

The certification body shall ensure that persons conducting QAMS auditing and conformity assessment have the knowledge corresponding to a post-secondary education that includes language and communications skills.

The certification body shall ensure that persons conducting QAMS auditing and conformity assessment have a minimum of five years' work experience in the PSC-related industry, including at least two years of work in quality assurance or risk management, or the equivalent. The number of years of total work experience may be reduced by one year if the person has completed appropriate and relevant post-secondary education.

The certification body shall establish, document, and maintain a process to evaluate and verify the training and competence of persons conducting QAMS auditing and conformity assessment, including appropriate continual training according to their specific qualification requirements to maintain competence.

NOTE: PSC-related industry experience may include security and human rights work experience.

7.3.7 Monitoring of Competence

The certification body shall ensure the acceptable performance of all personnel involved in its audit and conformity assessment activities. The certification body shall establish documented procedures and criteria for monitoring and measurement of the performance of all persons involved based on the frequency of their usage and the level of risk linked to their activities. The certification body shall review the competence of its personnel based on their performance in order to identify training needs.

The monitoring procedures shall include a combination of on-site observation, review of audit reports, and feedback from clients or other affected parties. Monitoring shall be designed in such a way as to minimize the disturbance of the normal processes of certification, especially from the client's viewpoint.

7.4 Use of Individual External Auditors and External Technical Experts

All the requirements from ISO/IEC 17021-1:2015, section 7.3, apply.

7.5 Personnel Records

All the requirements from ISO/IEC 17021-1:2015, section 7.4, apply. In addition, the following PSC-specific requirements apply.

The certification body shall maintain up-to-date records of relevant qualifications, training, experience, professional affiliations and memberships, professional status, and competence of all personnel involved in its audit and conformity assessment activities.

7.5.1 Background Screening and Appropriate and Relevant Security Clearances

Certification bodies shall establish, document, and maintain a procedure for screening and vetting of all personnel involved in its audit and conformity assessment activities. The certification bodies shall also ensure that all personnel involved in its audit and conformity assessment activities meet these requirements.

The process for security vetting and review of personnel involved in its audit and conformity assessment activities shall be documented in a way that can be accessed by organizations applying for conformity assessment and, where applicable, other relevant stakeholder organizations.

All personnel involved in its audit and conformity assessment activities shall be security cleared by their respective certification bodies. The vetting and clearance process shall include, but not be limited to, the following background checks, interviews, and review of work history.

7.5.1.1 Background Checks

Certification bodies shall carry out criminal, military, and human rights background checks of all persons working on behalf of the certification body assigned to perform QAMS audits and conformity assessment in accordance with data protection and privacy legislation. The checks are to include, as a minimum, a criminal records check (and for ex-services personnel, a military background check to ensure that the individual concerned has not been dishonorably discharged), as well as check personal and previous work references to ensure good conduct and ethical behavior consistent with respect for human rights. Where practicable, background checks shall be conducted through national agencies or authorities. Where this is not practicable, the certification body shall establish, document, and maintain a procedure to check suitability and integrity by an internal vetting process including records, checks, and interviews overseen by the organization's top management. The vetting process shall include review of documented submissions by the candidate, interviews, and reviews of documents such as passports, identity cards, work permits, driving licences, and workplace references.

7.5.1.2 Interviews

The certification body shall establish an interview procedure, including the hierarchy of interviewers, which shall be overseen by top management. Top management shall appoint a responsible manager who has been verified by interview and vetting as trustworthy and having the necessary competence and judgment to vet personnel involved in its audit and conformity assessment activities. The responsible manager shall assess through review of documentation submitted by candidates, and interviews and ongoing monitoring, the trustworthiness and appropriate behavioral characteristics of personnel involved in its audit and conformity assessment activities.

7.5.1.3 Work History

All personnel involved in its audit and conformity assessment activities shall provide evidence of at least five full years of continuous work history which shall be verified with current or previous employers. Self-employed candidates shall provide other appropriate documentation that demonstrates the same level of confidence and trustworthiness as employment records.

Candidates shall provide two work-related references, as well as one probity reference relevant to their work or local jurisdiction.

7.5.2   Credentials

All personnel involved in its audit and conformity assessment activities shall be issued tamper-resistant credentials with a unique number showing the following:

a)   Photograph;

b)   Full legal name;

c)   Period of validity; and

d)   Name, logo, and contact information of the certification body.

Credentials should be issued based on verifiable government issued identification.

7.5.3   Non-disclosure Agreements

All persons working on behalf of the certification body assigned to perform QAMS audits and conformity assessment shall sign confidentiality and non-disclosure agreements and a certification body code of ethics. The certification body shall establish, document, and maintain procedures on how to respect and protect the integrity of sensitive, confidential, and proprietary information. The certification body shall periodically review, as part of its own quality management system, the performance of its personnel with respect to taking appropriate steps to protect the sensitive, confidential, or proprietary information.

When requested, confidentiality and non-disclosure agreements signed by personnel involved in its audit and conformity assessment activities shall be made available to organizations undergoing conformity assessment.

7.5.4 Accountability

The certification body shall establish, document, and maintain procedures to make personnel involved in its audit and conformity assessment activities aware of infractions that could subject them to disciplinary actions, civil liability, and criminal prosecutions. The procedures shall include a process to address infractions of procedures, the code of ethics, and confidentiality and non-disclosure agreements, including investigation procedure and disciplinary actions. Records shall be kept of infractions, investigations, and any subsequent disciplinary actions.

7.5.5 Records

The certification body shall establish, document, and maintain procedures to maintain records of personnel involved in its audit and conformity assessment activities. Records shall be retained for periods that certification bodies deem appropriate and according to retention periods designated by national, international, and other legal requirements.

7.6 Outsourcing

All the requirements from ISO/IEC 17021-1:2015, section 7.5, apply.

8. INFORMATION REQUIREMENTS

All the requirements from ISO/IEC 17021-1:2015, section 8, apply. In addition, the following PSC-specific requirements apply.

The certification body shall establish, document, and maintain procedures that ensure a secure exchange of information regarding the functioning of the PSC's QAMS between the certification body, its client, and other parties that are permitted access to the information – such as the PSC's client. The certification body shall ensure that clients and other parties are aware of these procedures.

9. PROCESS REQUIREMENTS

All the requirements from ISO/IEC 17021-1:2015, section 9, apply, as well as guidance provided in the ISO 19011:2018. In addition, the following PSC-specific requirements apply.

9.1 General Requirements

The certification body shall precisely define the scope of certification in terms of the types of services the PSC provides and the geographic and technical areas of operations. The certification body shall not exclude part of the processes, sectors, products, or services from the scope of certification when those processes, sectors, products, or services have an influence on the delivery of services and demonstration of respect for human rights.

Risks are unique to each site; therefore, all sites included in an organization's scope of certification shall be subject to audit. The PSC organization shall have carried out a risk assessment for each site and shall implement risk treatments accordingly.

Sampling for organizations that operate multiple sites shall be based on a statistical risk-based approach, where the activities are substantially the same. Sites included in the scope of certification shall be audited, taking account of:

a) Reducing the duration of the audit for some sites where there is a similar risk profile or significantly reduced risk;

b) Consideration of special circumstances due to safety and security-related risks of either the certification body or PSC; and

c) Circumstances where the audit itself will create an intolerable risk for PSC operations.

In these cases, the certification body shall undertake a risk assessment and develop a risk-based audit program for the sites based on statistical sampling. This process shall ensure that a proper audit by the certification body of the PSC's QAMS is conducted. The process and special consideration in defining the scope of certification shall be justified and documented.

Where the certification body is certifying a multi-site organization under one certificate, the following conditions apply:

a) Consideration should be given for different legal jurisdictional areas;

b) All sites are operating under one centrally controlled and administered QAMS;

c) Internal audits are conducted on each site within the management system cycle;

d) Following certification, internal audits shall be carried out on each site within the certification period;

e) The internal audits of all sites shall demonstrate ongoing conformance to the ANSI/ASIS PSC.1-2012 (R2017) standard; and

f) Audit findings of the individual sites shall be considered indicative of the entire system and corrective and preventive actions shall be implemented accordingly.

9.2 Initial Audit and Certification

All the requirements from ISO/IEC 17021-1:2015, section 9.1, 9.2, and 9.3 apply. In addition, the following PSC-specific requirements apply.

9.2.1 Application

All the requirements from ISO/IEC 17021-1:2015, section 9.1.1, apply.

9.2.2 Application Review

All the requirements from ISO/IEC 17021-1:2015, section 9.1.2, apply. In addition, the following PSC-specific requirements apply.

Before commencing the audit, an agreement (see ISO/IEC 17021-1:2015, section 5.1.2) shall be established between the certification body and the applicant organization which:

a) Defines the scope of work to be undertaken, including the intended scope of certification and site details;

b) Establishes security, safety, and confidentiality arrangements;

c) Identifies subcontractors and supply chain partners included in the scope;

d) Identifies the security requirements of the client and persons being protected;

e) Requires the applicant organization to supply any information needed for its intended certification; and

f) Requires the applicant organization to comply with the requirements for certification.

The audit team shall be appointed (see ISO/IEC 17021-1:2015, section 9.2.2) and composed of auditors (and technical experts as necessary) who, between them, have the totality of the competences identified by the certification body (as set out in ISO/IEC 17021-1:2015, section 9.1.2.3) for the certification of the applicant organization. The selection of the team shall be based on the identification of the competence of persons conducting audit and conformance assessment made under Clause 7.2 of this *Standard* and may include use of both internal and external human resources. The audit team shall have the necessary competence, including sector or regulatory credentials, to determine whether the QAMS covers all the essential elements in a manner that gives adequate confidence that the system can be assured to meet specified requirements.

In certain instances, particularly where there are critical requirements and special procedures, the background knowledge of the audit team may be supplemented by briefing, specific training, or addition of non-auditor technical experts. If a certification body does use technical experts, its management control systems shall include documented procedures for selection and use of these experts, as well as evaluating and maintaining their competence. The certification body may rely on outside technical expertise – for example, from industry, human rights, or professional institutions. The certification body shall ensure that personnel providing technical expertise are bound by the same requirements as auditors for confidentiality and impartiality.

9.2.3   Initial Certification Audit

All the requirements from ISO/IEC 17021-1:2015, section 9.3, apply, as well as guidance provided in the ISO 19011:2018. In addition, the following PSC-specific requirements apply.

The objectives of the stage 1 audit are to provide a focus for planning the stage 2 audit by acquiring an understanding of the QAMS in the context of the organization's identified risks to quality assurance consistent with respect for human rights.

Stage 1 provides insight into whether the policy, risk assessment and objectives, and risk treatment methods have been effectively defined and interrelated to promote performance consistent with the ANSI/ASIS PSC.1-2012 (R2017) standard's requirements. The stage 1 audit shall collect and review necessary information within the scope of the QAMS, including but not limited to:

a)   Context of the organization and its operations;

b)   Clients' or other protected parties' needs and requirements;

c)   Supply chain and subcontractor node analysis;

d)   Risk assessment methodology, outcomes, and treatment methods;

e)   Human rights impact assessment, outcomes, and management methods;

f)   Services and geographical locations of the organization being audited;

g)   Related legal, regulatory, and contractual requirements of the applicant organization's operation;

h)   Validation that risk treatment, implementation, incident management, and evaluation programs address the issues identified in the policy, risk assessment and objectives;

i)   Documentation that QAMS documents and arrangements are in place for communication and consultation with internal and external stakeholders;

j)   Documentation that QAMS documents and arrangements are in place for human resource management (e.g., vetting and training personnel);

k)   Evidence of management commitment, review, and continual improvement;

l)   Risks introduced by the stage 2 audit process to the organization, its clients, and persons being protected; and

m)   Justification whether to proceed to the stage 2 audit.

Any part of the QAMS that is audited during the stage 1 audit and determined to be fully implemented, effective, and in full conformity with requirements of the ANSI/ASIS PSC.1-2012 (R2017) standard may not need to be re-audited during the stage 2 audit, as long as the certification body ensures that the already audited parts of the QAMS continue to conform to the certification requirements. In this case, the stage 2 audit report shall include these findings and clearly state that conformity has been established during the stage 1 audit.

Stage 2 audits shall have an audit plan (see ISO/IEC 17021-1:2015, section 9.2.3). The audit team shall conduct the stage 2 audit to gather audit evidence that the QAMS conforms to the ANSI/ASIS PSC.1-2012 (R2017) and other certification requirements. The audit and conformity assessment process shall audit and evaluate a sufficient number

of examples of activities of the client organization, using a documented sampling technique in relation to the QAMS to get a representative and accurate appraisal of the implementation and effectiveness of the QAMS. As part of the audit, the audit team shall interview a statistically representative number of the persons working on behalf of the organization, including top management and operational personnel of the audited facility, to provide assurance that the system is implemented and understood throughout the client organization.

The audit team shall analyse all information and audit evidence gathered during the stage 1 and stage 2 audits to determine the extent of fulfilment of all certification criteria of the ANSI/ASIS PSC.1-2012 (R2017) standard and identify any nonconformity – the absence of, or the failure to implement and maintain, one or more QAMS requirements or a situation which would, on the basis of available objective evidence, raise significant doubt about the efficacy of the organization's risk treatment plans and their ability to conduct their business consistent with respect for human rights. The audit team may suggest opportunities for improvement but shall not recommend specific solutions.

9.3   Surveillance Activities

All the requirements from ISO/IEC 17021-1:2015, section 9.6.2, apply. In addition, the following PSC-specific requirements apply.

The certification body shall have an established program for carrying out periodic surveillance audits at sufficiently close intervals to confirm that the certified QAMS continues to fulfil all certification requirements and to be effective. Surveillance audits shall be conducted at least once a year. The date of the first surveillance audit following initial certification shall be no more than 12 months from the last day of the stage 2 audit. The schedule for the surveillance audits, following initial certification, shall be determined at the end of the initial audit closing meeting.

The scope and frequency of surveillance audits shall take into account:

a)   The level of risk to the PSC and its stakeholders such as PSC clients, subcontractors, and impacted communities;

b)   The complexity of the PSC's operations;

c)   The nature of the operational environment;

d)   Concerns about the ability of the risk treatment programs to minimize undesirable and disruptive events;

e)   The size of sampling during the audit;

f)   Frequency and reports of incidents and complaints;

g)   The number of nonconformities observed at previous audits; and

h)   Changes in the organization, products, services, processes, or operating environment.

When, during a surveillance audit, instances of nonconformity or lack of evidence of conformity are identified, the certification body shall define time limits for correction and the corrective actions to be implemented. The audited organization shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future surveillance audits) will be needed to ensure effective correction and corrective actions. This decision will be based on the types and number of nonconformities identified.

9.4   Recertification

All the requirements from ISO/IEC 17021-1:2015, section 9.6.3, apply. In addition, the following PSC-specific requirements apply.

The recertification audit shall include an on-site audit. The recertification audit shall address the effectiveness of the QAMS in its entirety in the light of internal and external changes, including:

a) Changes in risk profile;

b) Changes in the context of the organization's operations;

c) Review and verification of the continued effective implementation of corrective action for every nonconformity from the previous audit;

d) The effective interrelationship between the elements of the QAMS; and

e) The fulfilment of ANSI/ASIS PSC.1-2012 (R2017) requirements.

NOTE: Factors taken into account as described in Sections 9.2.3 and 9.3 of this *Standard* apply.

9.5   Special Audits

All the requirements from ISO/IEC 17021-1:2015, section 9.6.4, apply.

NOTE: Factors taken into account as described in Sections 9.2.3 and 9.3 of this *Standard* apply.

9.6   Suspending, Withdrawing, or Reducing the Scope of Certification

All the requirements from ISO/IEC 17021-1:2015, section 9.6.5, apply.

9.7   Appeals

All the requirements from ISO/IEC 17021-1:2015, section 9.7, apply.

9.8   Complaints

All the requirements from ISO/IEC 17021-1:2015, section 9.8, apply.

9.9   Client Records

All the requirements from ISO/IEC 17021-1:2015, section 9.9, apply. In addition, the following PSC-specific requirements apply.

The certification body shall establish, document, implement, and maintain procedures to protect the integrity and security of clients' documents and records of a private, security sensitive, or proprietary nature, as well as the information and data derived from audits such as auditors' notes. The procedure shall describe how the documents are classified, accessed, handled, transported, archived, and subsequently destroyed consistent with their security, confidentiality, and privacy classification. Documents of any form or type of medium as well as data and records of a private, security sensitive, or proprietary nature shall be accessible only to designated persons with an appropriate level of security clearance working on behalf of the certification body who have signed non-disclosure agreements.

10.   MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES

All the requirements from ISO/IEC 17021-1:2015, section 10, apply.

10.1   Options

10.1.1 Option A: General Management System Requirements

All the requirements from ISO/IEC 17021-1:2015, section 10.2, apply.

10.1.2 Option B: Management System Requirements in accordance with ISO 9001

All the requirements from ISO/IEC 17021-1:2015, section 10.3, apply.

Annex A

(NORMATIVE)

A. REQUIRED KNOWLEDGE AND SKILLS

All the requirements from ISO/IEC 17021-1:2015, Annex A, apply.

This table provides additional areas of knowledge and skills in Annex A of ISO/IEC 17021-1:2015. The following table specifies the knowledge that a certification body shall define for specific certification functions.

X means the certification body shall define the criteria and depth of knowledge.

X+ indicates a need for deeper knowledge.

Table A.1: Table of Knowledge and Skills

Knowledge and skills	Certification functions		
	Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	Reviewing audit reports and making certification decisions	Auditing and leading the audit team
Management system knowledge and skills (7.3.2)	X	X	X+
Applicable laws, regulations, and other requirements relevant to the discipline (7.3.4)	X	X	X+
Understanding the requirements of the ANSI/ASIS PSC.1-2012 (R2017) quality assurance management system standard (7.3.5a)	X	X	X+
Understanding the requirements, roles, and responsibilities of PSC clients, government, and subcontractors (7.3.5b)		X	X
Managing the risks of undesirable and disruptive events (assess, anticipate, avoid, prevent, protect, mitigate, respond to, and recover) (7.3.5c)		X	X+
Knowledge of human rights and IHL, and the role of human rights and IHL non-governmental organizations (7.3.5d)		X	X
Terminology, processes, science, and technology relevant to the PSC sector (7.3.5e)		X	X
Terminology, practice, and understanding of the rule of law and use of force including those concerning weapons training and handling, security measures, personnel protection, and apprehension of persons (7.3.5f)		X	X
Measures for personal safety and security in theaters of operation (7.3.5g)			X
Methods for information gathering and monitoring (7.3.5h)			X

Knowledge and skills	Certification functions		
	Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	Reviewing audit reports and making certification decisions	Auditing and leading the audit team
Human rights impact assessment and risks related to protection of human rights (7.3.5i)		X	X+
Risk assessment (asset identification and valuation; risk identification, analysis, and evaluation) related to tangible and intangible assets (7.3.5j)		X	X+
Risk treatment (minimize likelihood and mitigate consequences) (7.3.5k)			X
Knowledge of incident communications and reporting protocols (7.3.5l)			X
Methods and practices for information integrity and sensitivity (7.3.5m)			X
Methods for personnel security and protection of persons (7.3.5n)			X
Methods and practices for asset protection and physical security (7.3.5o)			X
Methods and practices for avoidance, prevention, and deterrence management (7.3.5p)			X
Methods and practices for incident mitigation, preparedness, response, and crisis management (7.3.5q)			X
Methods and practices for continuity, emergency, and recovery management (7.3.5r)			X
Methods and practices for monitoring, measuring, and reporting of performance (including exercise and testing methodologies) (7.3.5s)			X

Expertise needs to exist within that team or should be supplemented by a technical expert when necessary. Where any audit is conducted by a team, the level of skills required should be held within the team as a whole and not by every individual member of the team.

Annex B

(INFORMATIVE)

B.1   Bibliography

ISO 31000:2009, Risk management – Principles and guidelines. Available at < http://www.iso.org >.

B.2   References

UN Guiding Principles on Business and Human Rights. Available at < https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. >.

ISO 18788:2015, Management system for private security operations – Requirements with guidance for use. Available at < http://www.iso.org >.

This page intentionally left blank

![ASIS International — Advancing Security Worldwide®]

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, Virginia 22314-2882
USA

+1.703.519.6200
Fax +1.703.519.6299
asisonline.org

Founded in 1955, ASIS International is the world's largest membership organization for security professionals. With hundreds of chapters across the globe, ASIS is recognized as the premier source for learning, networking, standards, and research. Through its board certifications, award-winning *Security Management* magazine, and the Global Security Exchange—the most influential event in the profession—ASIS ensures its members and the security community have access to the intelligence and resources necessary to protect their people, property, and information assets. Learn more about the work we do at asisonline.org.