CIS 10

Edition 1 September 2016

UKAS Guidance for Certification Bodies Certifying the Management Systems of Private Security Companies against ANSI/ASIS PSC1: 2012 or ISO 18788: 2015

United Kingdom Accreditation Service, 2 Pine Trees, Chertsey Lane, Staines-upon-Thames, TW18 3HR
Website www.ukas.com Publications requests Tel: 01784 429000 email: info@ukas.com

Contents

1. Introduction

This document provides guidance on the requirements and technical competences set out in ISO/IEC 17021-1 and ANSI/ASIS PSC 2 where appropriate for bodies seeking UKAS accreditation to certify to the American national standard ANSI/ASIS PSC1 or to ISO 18788 for private security companies (PSC).

2. Background

ANSI/ASIS PSC1 was developed as an American national standard in response to the requirement in the International Code of Conduct for Private Security Service Providers (ICoC) for objective and measurable standards for the provision of security services based on that code. The UK Foreign and Commonwealth Office decided in December 2012 to endorse PSC1 as the applicable standard against which UK based PSCs working in complex environments on land overseas might be certified.[1] The International Standards Organisation (ISO) developed and published ISO 18788 in 2015.

3. Accreditation

3.1 Certification bodies will be accredited by UKAS to certify to PSC1 and/or ISO 18788 using ISO 17021-1 as the accreditation standard.[2]

3.2 The accreditation assessment will include an assessment of the documentation of the certification body, an assessment at the offices of the certification body and the observation of

[1] Written Ministerial statement to Parliament of 17 December 2012 by Mr Mark Simmonds MP, Parliamentary Under Secretary of State

[2] ANSI/ASIS PSC2 provides background and guidance for certification bodies seeking accreditation to certify to PSC1.

at least one audit by the certification body to determine that the necessary systems have been effectively implemented, that the accreditation requirements have been met and that the certification body is competent to audit and certify to PSC1 and /or ISO 18788. The audits observed will need to cover both certification standards or if only one is covered the competence of the certification body for the other standard will be established through assessment at the offices of the certification body. This may include a Post Audit Review (see UKAS publication C1 General Principles for the Assessment of Management System, Product and Persons Certification Bodies). Any extra cost associated with the assessment, for instance as regards the need for Technical Expert support, specialised insurance and visas will be charged to the certification body (see UKAS standard terms and conditions).

3.3 Accreditation will be maintained through annual surveillance assessments and reassessment every fourth year. These assessments will include visits to the offices of the certification body and the observation of at least one audit of a PSC by the certification body each year. The audits observed will need to cover each certification standard over the four year accreditation cycle.

4. Initial Audit and Scope of Certification

Since PSC and other organisations seeking certification under PSC1 and/or ISO 18788 operate at multiple sites, certification bodies seeking accreditation need to determine and set out in a legally enforceable contract those management, geographic and technical services and sites to be covered by the certification; this forms the scope of certification. Any such area or site that contributes to the delivery of the core service against which the client of the certification body is to be certified shall be included in the Stage 2 audit, except where sampling is agreed by virtue of similar risks, management control and operations. IAF MD1 Certification of Multisite Sites Based on Sampling provides further guidance. Sampling of sites should take into account the specific circumstances posed by the safety and security related risks to the Certification Body, PSC, the PSC's client the local community and circumstances where the audit itself will create an intolerable risk to PSC operations. The certificate issued by the CB will identify the technical services, sites and geographic areas that are certified. (Despite the title certification to PSC1 would not be regarded by UKAS as equivalent to accredited certification against a quality management standard such as ISO 9001).

5. Requirements for Certification Bodies

PSC1 and ISO 18788 cover a wide range of specialist areas. This Guidance takes account of the pilot assessments carried out by UKAS, and identifies particular aspects in conjunction with the areas covered in ISO 17021-1 that need attention by the certification body, its audit team and subject matter experts.

In particular, the following areas require specialist preparation and expertise by the certification body:

- Situational awareness and the management of risk in complex environments and high risk areas
- International legal considerations and national regulatory and licensing requirements
- Contractual and insurance requirements
- Recruitment, training and vetting of security operatives, subcontractors and outsourced services
- Command and control arrangements, including liaison with international, national and local agencies

- Competence of key personnel in the security management system
- Code of ethics, respect for human rights, and voluntary commitments such as the ICoC and its Association[3] and the UN Guiding Principles for Business and Human Rights
- The procurement, licensing, usage, storage, import, export, trade (trafficking and brokering) movement and disposal of firearms and other controlled goods
- Competence in the use and selection of specialist security equipment including firearms and technology
- Guidance on rules for the use of force
- Incident management and reporting and the preservation of evidence
- Certification body insurance implications (including potential professional liability for complex environments, circumstances of war and terrorism, and medical and repatriation of personnel) and visa access requirements for the theatres in which it delivers services to clients

In keeping with 7.1.4 of 17021-1, the certification body shall have access to the necessary technical expertise for advice on matters directly relating to certification for technical areas, types of management system and geographic areas in which the certification body operates. Such advice may be provided externally or by certification body personnel. The certification body will need to demonstrate that it has the ability to identify, select, supervise, train, evaluate and authorise auditors and technical experts and to assess their initial and ongoing competences in the full range of specialist requirements for PSC certification, noting the fluid nature of complex environments. Auditors and experts should receive an up-to-date set of documented procedures giving audit instructions and all relevant information on the certification activities. These should include any known adjustments to the legal or PSC operating requirements in sample locations and any potential risk identification likely to be generated as a result of the auditing process (eg emergency security risk; in-country movement etc).

The audit team should determine whether the local personnel have fully understood the requirements of PSC1 and/or ISO 18788. This may require the services of an independent interpreter.

6. Auditor Competence

The range of knowledge required by the audit team, whether as an individuals or collectively as a team, should encompass the external standards and guidelines to be covered by the required certification and any voluntary commitments, in particular relating to human rights. At the heart of the PSC 1 and ISO 18788 standards is risk management which must be seen in the context of the often volatile environment in which PSCs operate. Risk management (for example as set out in ISO 31000) should be thoroughly understood by the auditors and certification decision makers. In addition to the required competence in risk and quality management, the audit team should have the requisite expertise and be trained to be able to cover the areas set out below:

a) Situational awareness and the management of risk
Including:

- Operational context including internal and external interested parties
- Risk analysis, including capability to assess and respond adequately and proportionately to any potential threat or change of circumstances, including possible non-compliance with legal and

[3] The International Code of Conduct for Private Security Service Providers (ICoC) -2010 and any amendments or interpretative guidance as may be issued by the International Code of Conduct Association.

regulatory requirements, fresh demands from the client, potential impact on internal and external interested parties, impacted people and organisations/communities (internal and external to the PSC)

Examples may include the implications of political flux, assurance and control in the supply chain, allegations of improper conduct or human rights abuse along with appropriate recourse to remedial action, the possibility of inappropriate use of force (not limited to the use of firearms), accidental discharge of a weapon, as well as a failure to comply with applicable laws and regulations in multiple jurisdictions – including the implications of weak host nation governance, and the brokering of controlled goods.

b) International and national regulatory and licensing requirements

Including:

- Awareness of multi-jurisdictional legal requirements, eg home states, contracting state, and host states
- Awareness of the regulatory and licensing requirements of the applicable jurisdictions, covering the trade (trafficking and brokering) movement, import/export of firearms, dual-use goods or other controlled goods (including ammunition, optics, helmets and body armour)
- Awareness of the requirements of the home state and host state eg as regards holding a current operating licence, the implications of Joint Ventures, and the recruitment and vetting of security operatives who may be carrying firearms overseas
- Awareness of the regulatory and licensing requirements and implications placed on PSC personnel by their home state and possible compliance mechanisms
- Awareness of the applicable Conventions and Codes
- Knowledge of UN Security Council, or other applicable International organisations' (e.g. EU) resolutions or relevant national legislation, relevant to anti-piracy operations, including those imposing sanctions and legislation giving effect to such sanctions. Ability to audit the adequacy and appropriateness of legal advice to PSC to ensure that it is operating within the bounds of international law and national regulatory requirements
- Knowledge of appropriate bribery, corrupt practices, and people trafficking and slavery legislation and regulations
- Data Protection legislation and possible compliance mechanisms

c) Human Rights

Human Rights is an integral part of risk management for a PSC and a core part of both PSC 1 and ISO 18788[4]. PSCs seeking to be certified to PSC1 or ISO 18788 must respect the human rights of those impacted by the PSCs operations, including by conforming to the Codes and commitments to which it subscribes such as the ICoC obligations and the UN Guiding Principles on Business and Human Rights, and with the applicable relevant obligations and laws.

To be able to audit effectively against this standard certification bodies may use either human rights technical experts or auditors with competence in human rights, or a mixture of both.

The competence required must cover human rights or if the expert is primarily expert in international humanitarian law, demonstrate additional competence in human rights and should include, at a minimum, knowledge and understanding of:

[4] Human Rights and International Humanitarian Law are complementary but IHL is limited in its application to situations of armed conflict.

- International human rights agreements relevant to PSCs, including the International Bill of Rights[5], the ILO Declaration on the Fundamental Principles and Rights at Work, the UN Guiding Principles on Business and Human Rights (UNGPs), and the International Code of Conduct for Private Security Service Providers
- How human rights risks and impact assessments methodology contributes to the overall PSC risk management approach
- The corporate responsibility to respect human rights, including as reflected in the UNGPs and their elaboration of human rights policy commitment, due diligence and corporate and operational level grievance and remedy mechanisms
- Practical application of the UNGPs to the private security sector including identifying and addressing human rights risks within the overall risk management approach
- Key human rights risks relevant to PSCs and stakeholders, including risks to its personnel and individuals/communities impacted by its operations. This will include, but not necessarily be limited to, risks related to the rights to life, liberty and security of the person, freedom from torture, cruel, inhuman or degrading treatment or punishment, freedom from slavery, forced and bonded labour, human trafficking, sexual abuse and harassment, rights to fair and just conditions of work, freedom of association, freedom from discrimination in employment and other labour rights including child labour
- Relevant regional and/ or home and host country human rights obligations
- Expected content of a PSC Code of Ethics (re PSC1, 9.1.2, ISO 18788, 8.2)

Human rights is a new area for approved industry standards, therefore if a certification body provides training to its auditors, it is especially important that this training should be robust and of a sufficient duration to cover the whole range of topics in this guidance. The evaluation of the competence of an auditor (see ISO 17021-1, 7.1.3) shall include human rights. Certification bodies may also choose to use a combination of approaches, with training supplemented by the contracting of a human rights expert or a human rights technical expert as required. The approach used should enable auditors to gain an in-depth understanding of the effectiveness of a PSCs respect for human rights throughout their functions.

d) Contractual and insurance requirements

Including:

- Typical commercial contracts; arrangements for legally enforceable contracts (including insurance cover) with subcontractors and outsourced activities providers; insurance requirements to cover the requirements of PSC contracts (state and non-state clients) including the area of operations
- Checking validity of insurance, including declared numbers of personnel/man-days (or other metric as appropriate), services delivered, jurisdictions and premiums being up to date
- Legal enforceability of contracts, eg state immunity where the contract is with a government agency
- Knowledge of the insurance required as an auditor operating in complex environments

[5] Comprising the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (IESCR).

e) Selection, recruitment and vetting of security operatives, subcontractors and outsourced services

Including:

- Methods of establishing that individuals have no criminal records
- Methods of establishing that individuals have the claimed experience and necessary competence and have not been involved in operations that have drawn allegations of human rights abuse or violations of international humanitarian law
- Vetting of staff from subcontractors and companies providing outsourced services[6]
- Vetting of outsourced suppliers to ensure they comply with relevant legal and regulatory codes to which the PSC is obligated

f) Training of security operatives and subcontracted personnel

Including:

- Auditing of training in command and control
- Auditing of training to ensure that all the requirements of PSC1/ISO 18788 are covered, including training provided by through a sub contracted body
- Training needs that cover the generic role of the PSC, the particular circumstances of contracts and requirements of clients, responsibility to the local community, the legal environment and respect for human rights and actions required where there are breaches of the company's policies and Code of Ethics and grounds for grievance and dismissal
- Ability to judge whether training is credible and effective

g) Command and control arrangements

Including:

- Contractual relationships, including client of the PSC, bridging agreements, joint venture management, command and control exercises, and contingency planning
- Chain of command, including in the event of absence or casualty
- Impact of changed circumstances, eg which might require rapid evacuation of the client
- Role and interaction with national and local agencies
- Communication of chain of command to PSC client

h) Law enforcement support operations and detainees

Including:

- Relevant state laws
- Responsibility of PSC under a contract in relation to any law enforcement support role, and detaining persons
- Reporting details of any person handed over to state authorities for detention
- Relevant international laws, including IHL (where applicable) and human rights law

If a PSC contract involves support to law enforcement operations, a certification body may wish to utilise an expert with experience to provide advice on this acutely sensitive area where there have been well established cases of past inhumane treatment breaching both criminal and human rights law.

[6] British Standard 7858 provides for the screening of security operatives.

i) Cultural issues
Including:
- Local mores, cultural and religious sensitivities in countries in which a PSC may operate

j) Training in the use of firearms, and care and maintenance
Including:
- Ability to judge whether the SOPs, qualifications of trainers, maintainers, structure of any course and training records and refresher training are satisfactory
- Awareness of any home, contracting or host state requirements for the recruitment, training and vetting of individuals carrying arms or ammunition overseas
- Awareness of the selection, acquisition, storage, cleaning, care and maintenance (both routine and periodic) and disposal of firearms, and ammunition
- Recording of incidents, including accidental discharges

k) Use of security technology
Including
- The use, maintenance and licensing of any security technology including tracking systems for personnel and assets, video cameras, video analytics, data storage and collection and for the confidentiality of any data
- Training in the use of security technology

l) Data retention and storage
Including:
- Secure data storage and retention periods[7]

m) Incident management and control and protection of evidence
Including:
- Guarding against contamination of incident sites
- Securing witness statements, for use in judicial or other authorised investigation
- The ability to manage and control the impact of an incident and record developments, including the ability to cope with most foreseeable (and some unforeseeable) eventualities
- The need for appropriate transparency and accountability in response including appropriate reports to interested parties
- Recording of incidents relating to possible allegations of human rights abuse and the preservation of any evidence of such incidents

n) Guidance on rules for the use of force (RUF)
Including:
- RUF, eg escalatory approach, use in self-defence, and use of force in support of law enforcement
- Legal review of policies and procedures
- Legislation of states in which a PSC may operate and international law, including where relevant International Humanitarian Law
- Existing guidance and best practice for RUF
- Need for procedures, training and refresher training

[7] Para 53 of ICoC requires employment and service records and reports to be held for a period of 7 years.

7. Confidentiality

In order to gain access to commercially privileged information, the certification body must undertake (in a legally enforceable contract) to hold confidential any sensitive, proprietary and or vulnerability information it acquires during an audit.

8. Decisions on Certification

The certification body retains authority and is responsible for its decisions relating to certification including the grant, maintenance, renewing, extension, reduction and withdrawal of certification.

9. Surveillance and Reassessment Procedures/Special Audits

The Certification Body shall carry out periodic surveillance and reassessment at sufficiently close interval to verify that the company or organisation whose management systems have been certified continues to comply with the certification requirements, noting the fluid nature of complex environments. Normal surveillance audits would take place at least yearly and recertification after three years. In the event of serious allegations being made against a company, the Certification Body may decide to conduct more frequent or special audits to maintain confidence.

10. Suspension, Withdrawal or Reducing Scope of Certification

Under the terms of ISO 17021-1, 9.6.5, the certification body is required to have a policy for suspension, withdrawal or reduction of the scope of the certification. This should apply when the company or organisation has seriously failed to meet certification requirements, including as regards any allegations of human rights abuse which have not been addressed, for which no or superficial grievance procedure has been instituted or where the company has been found to be legally liable. Depending on whether the alleged incident is local and limited, or more far reaching, the certification body will have a policy also to reduce the scope of the certification accordingly within a particular time frame.

11. References

1. ANSI/ASIS PSC1: 2012 - Management System for Quality of Private security Operations - Requirements with Guidance
2. ANSI/ASIS PSC2: 2012 - Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations
3. ISO 18788: 2015 - Management system for private security operations - Requirements with guidance for use
4. ISO/IEC 17021-1: 2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements
5. ISO 31000:2009: Risk Management - Principles and Guidelines
6. UN Universal Declaration of Human Rights 1948
7. The Geneva Convention relative to the Treatment of Prisoners of War and the Geneva Convention relative to the Protection of Civilian Persons in Time of War, 1949 and Additional Protocols
8. The Montreux Document - 2009
9. Guiding Principles on Business and Human Rights - Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011
10. The International Code of Conduct for Private Security Service Providers, 2010 and the International Code of Conduct Articles of Association, 2013
11. BS ISO 26000:2010 - Guidance on Social Responsibility
12. Voluntary Principles on Security and Human Rights 2000
13. UKAS publication C1 - General Principles for the Assessment of Management System, Product and Persons Certification Bodies, 2014