UKAS
A world of confidence

CIS 9

Edition 3 June 2024

UKAS guidance for Certification Bodies certifying private maritime security companies against ISO 28000/ISO 28007-1:2015

Contents

Changes since last edition

References to standards updated. Other minor editorial changes.

1. Introduction

This document provides guidance on the requirements and technical competences set out in ISO/IEC 17021-1 and ISO 28003:2007 for Certification Bodies seeking accreditation to certify to ISO 28000: 2022 using ISO 28007-1:2015 “Ships and marine technology – Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships, Part 1 General”.

2. Background

The first version of this standard, ISO PAS 28007, was commissioned by a UN Specialised Agency - the International Maritime Organisation (IMO) in May 2012. IMO specified that the scope of the ISO work should be bounded by their Interim Guidance document for MSC/1443.[1] Following international consultations, ISO PAS 28007 was submitted back to the IMO Maritime Safety Committee in November 2012 for approval, and then published by ISO in December 2012. ISO PAS 28007 was revised and published as ISO 28007-1 in April 2015.

[1] Interim Guidance to Private Maritime Security Companies Providing Private Contracted Armed Security Personnel on Board Ships in the High Risk Area MSC1/Circ.1443 25 May 2012

3. Accreditation

Certification Bodies will be accredited by UKAS to certify to ISO 28000/ISO 28007-1 using ISO/IEC 17021-1 as the accreditation standard in conjunction with ISO 28003.

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 at least one audit of a PMSC 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 ISO 28000/ISO 28007-1. Any extra costs 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 of business).

Accreditation will be maintained through annual surveillance assessments and reassessment every fourth year. Based on conformance risk of the Certification Body, these assessments will include visits to the offices of the Certification Body, and the observation of at least one audit of a PMSC by the Certification Body each year.

4. Initial audit and scope of certification

ISO 28007-1 provides sector specific guidance to PMSC seeking certification under ISO 28000. It covers the operations of PCASP on board ships. It provides additional guidance to support the development of the security management system, supply chain and logistic support systems which are established through ISO 28000. It does not address the provision of other security services in the maritime space such as security consultancy or training for State entities.

There is a recommendation in the scope of ISO 28007-1 that the certificate contain the words: “This certification has been prepared using the full guidelines of ISO 28007-1 as a Private Maritime Security Company providing Privately Contracted Armed Security Personnel”. The certification of the management system is to ISO 28000, with the above text to be included on UKAS accredited certification.

Many shipping companies privately contract armed guards to be stationed on board ships going through the area formerly known as the High Risk Area of the Indian Ocean[2] or other areas where there is a serious security threat. In order to sustain such security support, PMSC routinely operate in multinational jurisdictions across international boundaries. The management controls required may need different approaches depending on the local context. 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 certified; this forms the scope of certification. These need to be confirmed through the Certification Body’s application review process and the Stage 1 audit and covered by a Stage 2 audit. The audit confirms that the management system of the PMSC is capable of delivering to the ISO 28000 and ISO 28007-1 requirements for the scope of certification. Any nonconformities would be raised against ISO 28000, with reference to the relevant clause in ISO 28007-1. Any such geographic areas or sites that contribute to the delivery of the core service of armed guarding against which the PMSC is to be certified needs to be included, except where sampling is agreed by virtue of similar risks, management controls and operations.

[2] High Risk Area as a designation was removed by the Lloyds Market Association Joint War Committee on 1 January 2023

5. Requirements for Certification Bodies

ISO 28007-1 covers 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/IEC 17021-1 and ISO 28003 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;
- 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 and the role of the Master;
- competence of key personnel in the security management system;
- codes of ethics, respect for human rights, and voluntary commitments such as ICoC and its Association[3] and the UN Guiding Principles on 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 and technology;
- procedures and rules for the use of force;
- incident management and reporting and the preservation of evidence.

In keeping with 7.1.4 of ISO/IEC 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 competences in the full range of specialist requirements for PMSC certification. 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 maritime security operating framework and any potential risk identification likely as a result of the auditing process (e.g. pilot transfers, emergent security risk etc).

The audit team should determine whether personnel have fully understood the requirements of ISO 28007-1. This may require the services of an independent interpreter.

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

6. Auditor competence

The range of knowledge required by the audit team, whether as an individual 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 risks and impacts. At the heart of ISO 28000 lies risk management; this is more than 'threat management' and must be placed in the international context of the maritime industry. 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 (e.g. vessel diversion) including possible non-compliance with legal and regulatory requirements, fresh demands from the client, potential impact on internal and external interested parties (e.g. wounded or unauthorised person aboard or allegation of improper conduct or human rights abuse) or logistics problems.

b) International and national regulatory and licensing requirements:

Including:

- Awareness of multi-jurisdictional legal requirements, e.g. flag, coastal, home and port 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 regulatory and licensing requirements placed on PMSCs by their home state in relation to the trade (trafficking and brokering) or movement of controlled goods across international borders including the implications of potential insolvency, and use of vessel-based armouries.
- Awareness of the applicable Conventions and Codes including the UN Convention on the Law of the Sea (UNCLOS), the International Convention for the Safety of Life at Sea (SOLAS), the Convention for the Suppression of Unlawful Acts of violence against the Safety of Maritime Navigation (SUA) and the International Ship and Port Facility Security Code (ISPS Code)[4] and any relevant guidance issued by the International Maritime Organisation (IMO).
- 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.
- Awareness of any International sanctions as well as relevant national legislation giving effect to such UN/EU measures.
- Awareness of any home state requirements for licensing of individuals carrying arms overseas.[5]

[4] See Bibliography and also the guidance issued by IMO Maritime Safety Committee, especially MSC.1/Circ 1443 2012

[5] British regulatory requirements apply extraterritorially to British nationals as regards trafficking and brokering of controlled goods, including firearms i.e. arranging for firearms to cross borders/jurisdiction even if the company is not British but employs British nationals in a controlling role

c) Contractual and insurance requirements

Including:

- Typical commercial contracts. Arrangements for legally enforceable contracts (including insurance cover) with subcontractors and outsourced activities providers.
- Relevant insurance requirements to ensure that PCASP team and the PMSC client it supports are covered including maritime employers' insurance.
- Awareness of insurance premium payment framework for PMSCs to ensure cover is current and credible.[6]

d) Selection, recruitment and vetting of security operatives sub-contractors and outsourced services:

Including:

- PMSC employment models, including direct employment, subcontracting of individuals, out-sourcing through 2nd party human resource providers, partnering with other PMSCs – and how those arrangements influence training and human resource management.
- 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.
- Methods of reviewing the medical, physical and mental fitness of personnel.
- Data Protection legislation and possible compliance mechanisms.
- Vetting of staff from subcontractors and companies providing outsourced services.[7]
- Vetting of outsourced suppliers to ensure they comply with the relevant legal and regulatory codes to which the PMSC is obligated e.g. vessel-based armoury services (and their maritime legal and safety obligations).
- Home state requirements for licensing of security operatives who might be carrying firearms and other controlled goods on nationally flagged vessels or overseas.

e) Training of security operatives and sub-contractors:

Including:

- Auditing of training in command and control and the responsibility of the Master and the PCASP role.
- Auditing of training to ensure that all the requirements of ISO 28007-1 are covered, including any training provided through a subcontracted body.
- Training needs that cover the generic role of the PCASP, 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 dismissal.
- Medical training requirements applicable to PMSCs (an example is First Person On Scene).
- Ability to judge whether training is credible and effective.

[6] Premiums are generally paid every 45 – 60 days on the declared number of personnel at sea during that period. Premium payments need to be up to date.

[7] British Standard 7858 provides for the screening of security operatives. UK and Germany among others apply national requirements to the licensing of security operatives at sea.

f) Command and control arrangements:

Including:

- Chain of command, responsibility of PCASP team leader, responsibility of the Master.
- Coastal state jurisdiction.
- Flag state jurisdiction.

g) Human rights

Human Rights is an integral part of risk management and a core part of ISO 28007.[8] PMSCs seeking to be certified to ISO 28007-1 must respect the human rights of those affected by the PMSC's operations within the scope of ISO 28007-1, including by conforming with relevant legal and regulatory obligations and the UN Guiding Principles on Business and Human Rights.

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:

- International human rights agreements relevant to PMSCs, including the International Bill of Rights,[9] the ILO Declaration on the Fundamental Principles and Rights at Work and the UN Guiding Principles on Business and Human Rights (UNGPs).
- How to conduct human rights impact assessments and how an effective human rights impact assessment can contribute to the overall PMSC risk management approach.
- The corporate responsibility to respect human rights as defined in the UNGPs,[10] including its recommendations on human rights policy commitment, due diligence and operational level grievance mechanisms.
- Key human rights risks relevant to PMSCs and stakeholders, including risks to its personnel, others on board and others its personnel may come into contact with at sea or ashore. 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.
- Practical application of the UNGPs to the private maritime sector including identifying and addressing human rights risks within the overall risk management approach.
- Relevant regional and/or domestic human rights obligations and additional voluntary commitments to which a PMSC may subscribe including joining ICoCA.
- Relevant domestic human rights obligations as prescribed by the flag state (if applicable) of the vessel that the PMSC is servicing.
- Expected content and application of a PMSC Code of Ethics (re ISO 28007-1, 4.1.7).
- Third party complaints, grievance and whistleblowing procedures including issues around communication and transparency of procedures and appeal mechanisms.

[8] Human rights and International humanitarian law are complementary but IHL applies in situations of armed conflict.

[9] 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).

[10] "Companies should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved." (UNGP 11)

Human rights is a relatively 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/IEC 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 human rights technical expert as required. The approach used should enable auditors to gain an in-depth understanding of PMSCs respect for human rights throughout their functions.

h) Detainees and unauthorised persons

Including:

- Responsibility of the Master and of PMSC in relation to disarming persons.
- Responsibility of the Master in relation to the detention of persons.
- Relevant Flag and coastal state laws.
- Reporting details of any person handed over for detention.
- Relevant international laws, including IHL (where applicable) and human rights law

i) Training in the use of firearms, 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 state or flag state requirements for the recruitment, training and vetting of individuals carrying arms or ammunition overseas.
- Awareness of the selection, acquisition, storage, control, cleaning, care and maintenance (both routine and periodic), and disposal of firearms, and ammunition.
- Recording of incidents, including accidental discharges.

j) Use of security technology

Including:

- The use, maintenance and licensing of any security technology including tracking systems for personnel and assets, video cameras on board, video analytics, data storage and collection and for the confidentiality of any data.
- Training in the use of security technology.

k) Data retention and storage:

Including:

- Secure and lawful data storage and retention periods.[11]

l) Incident management and control and preservation of evidence:

Including:

- 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.

[11] Para 53 of ICOC requires employment and service records and reports to be held for a period of 7 years, ISO 28007-1 para 4.6.2 requires records to be held in keeping with applicable legislation and regulatory requirements.

- The need for transparency and accountability in response including full reports to interested parties, including insurers and owner/charterer.
- Recording of incidents relating to possible allegations of human rights abuse and the preservation of any evidence of such incidents.

m) Guidance on Rules for the use of force (RUF):

Including:

- RUF, e.g. escalatory approach, use in self-defence.
- Legal review of policies and procedures.
- Legislation of flag and coastal states and international law, including where relevant International Humanitarian law.
- Existing guidance and best practice for RUF.
- Need for procedures, training and refresher training.

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 recertification procedures/special audits

The Certification Body shall carry out periodic surveillance and recertification audits at sufficiently close interval to verify that the company or organisation whose management systems have been certified continues to comply with the certification requirements. 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 a special audit within a shorter timeframe. Where relevant, appropriate stakeholders should be informed.

10. Suspension, withdrawal or reducing scope of certification

Under the terms of ISO/IEC 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 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 timeframe.

References

1. ISO 28000: 2022 Security and resilience - Security management systems – Requirements
2. ISO 28003: 2007 Security management systems for the supply chain; Requirements for bodies providing audit and certification of supply chain security management systems
3. ISO/IEC 17021-1: 2015 Conformity Assessment – Requirements for bodies providing audit and certification of management systems
4. ISO 31000:2018 Risk Management – Guidelines
5. UN Convention on Law of the Sea (UNCLOS) 1982
6. The International Code of Conduct for Private Security Service Providers 2010 as amended 10 December 2021 and the International Code of Conduct Articles of Association 2013 as amended 5 December 2023
7. UN Guiding Principles on Business and Human Rights 2011
8. UN Universal Declaration of Human Rights 1948
9. UN General Assembly Resolution 72/180 (2018) (protection of human rights while countering terrorism)
10. Protocol to the UN Convention for the Protection of Unlawful Acts against the safety of Maritime Navigation, 2009
11. International Convention for the Safety of Life at Sea, SOLAS (1974)
12. Convention for Suppression of Unlawful Acts of Violence against the Safety of Maritime Navigation (SUA) 2005
13. International Ship and Port Facility Security Code (ISPS)