PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28007

First edition
2012-12-15

Ships and marine technology — Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships (and pro forma contract)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Navires et technologie maritime — Guide destiné aux sociétés privées de sécurité maritime (PMSC) fournissant des agents de protection armés embarqués sous contrat privé (PCASP) à bord de navires (et contrat pro forma)

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

Reference number
ISO/PAS 28007:2012(E)

© ISO 2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO 2012 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3079f5/iso-pas-28007-2012

© ISO 2012 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/...
ISO/PAS 28007-2012

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/PAS 28007 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

© ISO 2012 – All rights reserved

Introduction

ISO 28000 is the certifiable security management system for organizations which has been developed from other quality management systems (ISO 9001 and ISO 14001) with the same management system requirements.

In effect ISO 28000 is a risk based quality management system for the security of operations and activities conducted by organizations. ISO 28007 sets out the guidance for applying ISO 28000 to Private Maritime Security Companies (PMSC)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

© ISO 2012 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

Ships and marine technology — Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships (and pro forma contract)

1 Scope

This Publicly Available Specification gives guidelines containing additional sector-specific recommendations, which companies (organizations) who comply with ISO 28000 can implement to demonstrate that they provide Privately Contracted Armed Security Personnel (PCASP) on board ships. To claim compliance with these guidelines, all recommendations ("shoulds") should be complied with.

Compliance with this Publicly Available Specification can be by first, second and third party (certification). Where certification is used, it is recommended the certificate contains the words: "This certification has been prepared using the full guidelines of ISO PAS 28007 as a Private Maritime Security Company providing Privately Contracted Armed Security Personnel".

2 Normative references

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/77797865-1ea5-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

ISO 28000, *Specification for security management systems for the supply chain*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Private Maritime Security Company
PMSC
organization which provides security personnel, either armed or unarmed or both, on board for protection against piracy

Note 1 to entry: Henceforth throughout this document, the word "organization" refers to the PMSC.

3.2
Privately Contracted Armed Security Personnel
PCASP
armed employee or subcontractor of the PMSC

3.3
area of high risk of piracy
area identified as having an increased likelihood of piracy

3.4
guidance on the Rules for the Use of Force (RuF)
clear policy drawn up by the PMSC for each individual transit operation which sets out the circumstances in which lethal force in the delivery of maritime security services may be used in taking account of international law and the law of the flag state

© ISO 2012 – All rights reserved

3.5
International Code of Conduct for Private Security Service Providers (ICoC) (9 November 2010)
code that identifies a set of principles and processes for private security providers related to support for the rule of law and respect for human rights in the context of self-regulation by private security companies

Note 1 to entry: IMO has stated that ICoC is not directly applicable to the peculiarities of deploying armed guards at sea to protect against piracy since it is written in the context of self-regulation for land companies only.

3.6
interested party
person or organization that can affect, be affected by or perceive themselves to be affected by a decision or activity

Note 1 to entry: This denotes but is not limited to clients (ship-owners, charterers), the shipping community including seafarers, flag, coastal and port states, international organizations, P and I clubs and insurers, and security training companies, certification bodies.

3.7
maritime security services
services which range from intelligence and threat assessment to ship hardening and the guarding and protection of people and property (whether armed or unarmed) or any activity for which the Company Personnel may be required to carry or operate a firearm in the performance of their duties

3.8
Montreux document
document which reaffirms the obligations on states to ensure that private military and security companies operating in armed conflicts comply with international humanitarian and human rights law

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 1 to entry: IMO has similarly stated that because Montreux applies in situations of armed conflict, it is not relevant to the operations of piracy and armed robbery at sea.

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

3.9
personnel
persons working for a PMSC whether as a full time or part time employee or under a contract, including its staff, managers and directors

3.10
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73, definition 3.4.1]

3.11
firearms
portable barrelled weapon from which projectile(s) can be discharged by an explosion from the confined burning of a propellant and the associated ammunition, related ancillaries, consumables, spare parts and maintenance equipment used by security personnel at sea

3.12
security
process to pre-empt and withstand intentional, unauthorised act(s) designed to cause harm, damage or disruption

3.13
home state
state of nationality of a PMSC, i.e. where a PMSC is domiciled, registered or incorporated

3.14
coastal state
state of nationality of the area of transit within coastal waters, including nationality of ports visited

© ISO 2012 – All rights reserved

3.15
security management objective
specific outcome or achievement required of security in order to meet the security management policy

3.16
security management policy
overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and legal and regulatory requirements

3.17
security related equipment
protective and communication equipment used by security personnel at sea

3.18
supernumerary
status of PCASP contracted by PSMCs at sea that are neither regular crew nor passengers, are directed by a team leader and are under the overall authority of the Master of the ship

Note 1 to entry: Supernumeraries should be declared as such on a crew list.

3.19
team leader
designated leader of the personnel contracted to provide security services aboard the ship

3.20
threat assessment
assessment by the client, by the PMSC or by international experts and organizations on the potential risks from piracy or other dangers to a specific transit or to operations more generally

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-

3.21
top management
person or group of people who direct and control an organization at the highest level

4 Security management system elements for Private Maritime Security Companies

4.1 General requirements

4.1.1 Understanding the PMSC and its context

The organization should determine and document relevant external and internal factors. These include the international and national legal and regulatory environment including licensing and export/import requirements, the political, the natural and physical environment, the role, perceptions and risk tolerance of the client and other interested parties as well as key international developments and trends in the home state, flag and coastal states and areas of operation. The organization should also evaluate and document elements that might impact on its management of risk including its own organization and lines of authority for operations, its capabilities in delivering objectives and policies, and the contribution of partners and subcontractors. The evaluation should include the particular circumstances of each operation or transit and the attendant risk factors for the organization.

The organization should also incorporate and take notice and actions as necessary on the significant elements in the risk analysis of the ship-owner which has prompted consideration of the use of PCASP, and the legal requirements of the flag state and the need for prior approval to deploy PCASP. The organization should determine how this applies to its planning needs and expectations and that it is reflected in its own risk assessment. The organization should demonstrate its understanding of the interaction of these elements within its context.

© ISO 2012 – All rights reserved

4.1.2 Understanding the needs and expectations of interested parties

The organization should identify and maintain a register of the interested parties that are relevant to the organizations' operations and the related legal and regulatory requirements, taking account of the perceptions, values, needs, interests and risk tolerance of the interested parties.

It is important for the PMSC to understand that before contracting for their services, a ship-owner will have carried out a "risk assessment". The PMSC should then determine how this applies to them and demonstrate how it impacts on needs and expectations.

The organization should consider risk criteria that may impact on interested parties as follows:

a) the overall risk policy of the organization, and of the client, and their risk tolerance;

b) the inherent uncertainty of operating at sea in an area with high risk of piracy;

c) the nature of the likely threats and consequences of an incident on its operations, reputation and business;

d) the impact of an incident; and

e) the impact of the combination of a number of risks.

4.1.3 Determining the scope of the security management system

The organization should determine the boundaries and applicability of the security management system to establish its scope.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The scope should be available as documented information.

In addition to the security management systems requirements specified in ISO 28000, the organization should determine the scope of the security management system, including coverage of any subordinate bodies, regional bodies or subcontracted entities.

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/77707865-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

4.1.4 Security management system

The organization should establish, implement, maintain and continually improve a risk based security management system.

4.1.5 Leadership and commitment

Top management should demonstrate leadership and commitment with respect to the security management system by:

a) ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the security management system requirements into the organization's business processes;

c) providing sufficient resources to deliver, implement, review and continually improve the security management system;

d) communicating the importance of effective security management and of conforming to the security management system requirements;

e) compliance with legal and regulatory requirements and other requirements to which the organization subscribes;

f) ensuring that the security management system achieves its intended outcome(s);

g) directing and supporting persons to contribute to the effectiveness of the security management system;

© ISO 2012 – All rights reserved

h) promoting continual improvement;

i) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this Publicly Available Specification should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

4.1.6 Competence

Top management should demonstrate and document the skills and experience, and professional capability to provide the leadership and play their roles in oversight of security operations at sea and specifically the protection of persons aboard the ship against unlawful attack, using only that force which is strictly necessary, proportionate and reasonable. The organization should:

a) determine the necessary competence on the basis of qualifications, training and relevant and appropriate experience of person(s) doing work under its control that affects its security performance;

b) have established and documented procedures as regards leadership, chain of authority, change in command in the event of illness or incapacity of a key operational figure including the team leader and as regards life saving;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

d) have established procedures to develop guidance for the use of force based on the consideration of several scenarios and providing a graduated response plan;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

e) have a documented, robust and auditable health, safety and environmental policy;

f) have written testimonials from previous clients relating to the organization's delivery of its security performance at sea and/or in other relevant circumstances, where the company has a history of related service delivery;

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/7770f685-1ea3-4448-8a4d-ebd8fe3075f5/iso-pas-28007-2012

g) have a process for post incident actions to support state authority investigations/prosecutions should a formal investigation be required and;

h) retain appropriate documented information as evidence of competence.

4.1.7 Organizational roles, responsibilities and authorities

Roles, responsibilities and authority in the organization should be established and documented from top management to command and control of the PCASP, with a pre- established progression in lines of authority taking account of any possible absence or incapacity.

In providing maritime security, for personnel and assets as detailed in a contract, such as in Annex A or similar, such roles for the organization may include:

a) risk assessment and security advice for the client as to the most effective deterrent, whether armed personnel, ship hardening and/or technology or a combination of measures, whether in general or for a specific transit;

b) an intelligence assessment as to the evolving situation in the proposed area of operations;

c) observation and monitoring of activity in the operating area, including advice to the Master on routeing in the light of an evolving threatening situation;

d) deployment of PCASP;

e) responsibility for the embarkation, inventory, and secure storage of firearms and ammunition associated with the deployment of a PCASP;

© ISO 2012 – All rights reserved

f) security advice to the Master and under his authority, training of (non PCASP) personnel aboard in emergency procedures response to a threat, including recourse to a citadel;

g) first aid and casualty care and help with evacuation;

h) preservation of evidence and protecting a crime scene as far as practicable;

i) supporting the Master in reports to international liaison and flag state authorities;

j) supporting the master in reports to the client;

k) collation of post incident reports and the response made as a contribution to lessons learned;

l) robust arrangements for the provision of visas, travel documents and security identity documentation, as well as any necessary licences required.

All roles carried out by the organization and its PCASP should be as defined in the relevant documentation.

4.1.8 Culture and ethics

The organization should:

a) have an accessible, written Code of Business Ethics and Code of Conduct;

b) be able to demonstrate that personnel are conversant with its ethical policies, procedures and plans and that these are regularly reviewed and updated.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.1.9 Structure of the organization

The organization should have a clearly defined management structure showing control and accountability at each level of the operation which should:

ISO/PAS 28007:2012
https://standards.iteh.ai/catalog/standards/sist/777078b5-1ca3-4448-ba4d-ebd8fe3075f5/iso-pas-28007-2012

a) define and document ownership and a place of registration of the organization;

b) identify and document top management and their past history and relevant experience;

c) define and document that the organization is registered as a legal entity or part of a legal entity, and where appropriate, the relationship between the organization and other parts of that same legal entity;

d) define and document any subordinate bodies, regional offices, joint venture partners and their places of incorporation and relationship to the overall management structure; and

e) define and document any operational bases, logistics or storage facilities used in support of the operations of the organization and the jurisdiction that applies and/or whether they are on the high seas.

4.1.10 Financial stability of the organization

The organization should be able to demonstrate its financial stability, debt profile, any unserved criminal or fraud charges by its top management or other history that might impact on its operations and on interested parties.

The organization should be able to document its financial stability by way of:

a) latest financial accounts supplemented with management accounts;

b) banker's references or similar national equivalents as required;

c) company structure and place of registration;

d) company ownership.

© ISO 2012 – All rights reserved