INTERNATIONAL STANDARD

ISO 28007-1

First edition
2015-04-01

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) —

Part 1: General

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

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) —

Partie 1: Généralités

Reference number
ISO 28007-1:2015(E)

© ISO 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

© ISO 2015 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

© ISO 2015 – 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 28007-1 cancels and replaces ISO/PAS 28007:2012.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

Introduction

ISO 28000 is the certifiable security management system standard for organizations which has been developed along the format of other management system standards (ISO 9001 and ISO 14001) with the same management system requirements.

ISO 28000 was developed in response to demand from industry for a security management standard with the objective to improve the security of supply chains and is certifiable in accordance with the International Accreditation Forum. In effect ISO 28000 is a risk-based quality management system for the security of operations and activities conducted by organizations. Organisations seeking to be certified to this International Standard should respect the human rights of those affected by the organisations operations within the scope of this International Standard, including by conforming with relevant legal and regulatory obligations and the UN Guiding Principles on Business and Human Rights. This part of ISO 28007 sets out the guidance for applying ISO 28000 to Private Maritime Security Companies (PMSC).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

© ISO 2015 – All rights reserved

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) —

Part 1: **General**

1 Scope

This part of ISO 28007 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 part of ISO 28007 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 28007-1 as a Private Maritime Security Company providing Privately Contracted Armed Security Personnel”.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

2 Normative references

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 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 International Standard, the word “organization” refers to the PMSC.

3.2
Privately Contracted Armed Security Personnel
PCASP
armed employee or subcontractor of the Private Maritime Security Company (PMSC)

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

© ISO 2015 – All rights reserved

3.4
guidance on the procedures or rules for the use of force (RuF)
clear policy drawn up by the Private Maritime Security Company (PMSC) for each individual transit operation which sets out the circumstances in which force, to include 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

3.5
Security Management System
SMS
risk-based security framework

3.6
interested party and stakeholders
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, THE flag STATE, impacted communities, coastal 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
Guiding Principles on Business and Human Rights
UNGPs
guidance principles to companies on how to respect the human rights of all those affected by their operations, including developing a human rights policy, taking steps to identify, address and mitigate human rights risks and developing effective operational level grievance mechanisms

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

3.9
personnel
persons working for a Private Maritime Security Company (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 Private Maritime Security Company (PMSC), i.e. where a PMSC is domiciled, registered or incorporated

© ISO 2015 – All rights reserved

3.14
coastal state
state of nationality of the area of transit within coastal waters

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

3.19
threat assessment
assessment by the organization, the client and other expert sources on the potential for acts of piracy or other threats to a specific transit or to operations more generally

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.20
top management
person or group of people who direct and control an organization at the highest level

ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

3.21
incident
event that has been assessed as having an actual or potentially adverse effect

4 Security management system elements for Private Maritime Security Companies (PMSC)

4.1 General requirements

4.1.1 Understanding the PMSC and its context

The organisation 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, needs, expectations and risk tolerance of the client and other interested parties and stakeholders as well as key international developments and trends in the home state, flag and coastal states and areas of operation. The organisation should also evaluate and document elements that might impact on its management of risk including its own organisation and lines of authority for operations, its capabilities in delivering objectives and policies, and the contribution of partners and subcontractors, and any voluntary commitments to which the organisation may subscribe. The evaluation should include the particular circumstances of each operation or transit and the attendant risk factors for the organisation.

The organisation should also identify, document and manage as necessary the significant risks identified by the ship owner which have prompted consideration of the use of security services which may include PCASP. Where PCASP are used, this should cover the legal requirements of the flag state, and of the coastal state where applicable and relevant, and the need for prior approval to deploy PCASP. The organisation should determine how this applies to its planning needs and expectations and that it is reflected in its own risk assessment. The organisation should demonstrate its understanding of the interaction of these elements (within its context).

4.1.2 Understanding the needs and expectations of interested parties

The organization should identify and maintain a register of the interested parties and stakeholders 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 and stakeholders. As part of its own risk assessment process, the organization should carry out a meaningful consultation with relevant interested parties and stakeholders, including those directly affected by its operations.

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 and its own risk assessment.

The organization should consider risk criteria that may impact on interested parties and stakeholders 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ad3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

4.1.3 Determining the scope of the security management system

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

The scope should be available as documented information.

The scope of the security management system should include the security management system requirements specified in ISO 28000 and take into account any subordinate bodies, regional bodies and subcontracted entities that impact the delivery of security services.

4.1.4 Security management system

The organization should establish, implement, maintain and continually improve a security management system. Where the organization has an existing management system, it should ensure consistency in plans and practice across systems and avoid duplication wherever practicable.

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;

© ISO 2015 – All rights reserved

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 or voluntary commitments 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;

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 International Standard 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 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;

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b55efc1d/iso-28007-1-2015

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;

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;

g) have a process for post incident actions to support state authority investigations/prosecutions should a formal investigation be required and to support internal evaluation of performance as part of the continual improvement process;

h) retain appropriate documented information as evidence of competence.

4.1.7 Organizational roles, responsibilities and authorities

Roles, responsibilities and authority in the organisation should be established from top management down to those providing security services on or for a ship, including command and control of any PCASP and a pre-established progression in line of authority taking account of any possible absence or incapacity. Such roles 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) intelligence reporting regarding the status of commercial shipping, friendly forces, and possible hostile actors 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;

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

j) 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 organisation and its security personnel including any PCASP should be as defined in the relevant documentation, culture and ethics

The organization should:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) have an accessible, written Code of Ethics including its human rights policy and Code of Conduct;

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

ISO 28007-1:2015
https://standards.iteh.ai/catalog/standards/sist/ed3d2abf-36d1-40bc-93da-4a10b53efc1d/iso-28007-1-2015

4.1.8 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:

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.

4.1.9 Financial stability of the organization

The organisation should be able to demonstrate its financial processes, administrative procedures, or other relevant history that might impact on operations and interested parties and stakeholders. 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;

© ISO 2015 – All rights reserved