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

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)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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).

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".

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

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

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

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

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

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.

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;

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;

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:

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.

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;

d) company ownership.

4.1.10 Outsourcing and subcontracting

The organization should have a clearly defined and documented process to explain the circumstances under which it outsources activities, functions or operations and its supply chain. The organization should take responsibility for activities outsourced to another entity and have a legal enforceable agreement covering such arrangements including:

a) commitment by a subcontracted entity to abide by the same legal and regulatory obligations and equivalent Code of Ethics as the organizations, including those under this International Standard;

b) confidentiality and conflict of interest agreements;

c) the identification and documentation of its logistics chain and the risk potential from that logistics chain including arrangements for the licensing and export/import of firearms and security material.

4.1.11 Insurance

The organization should demonstrate that it has sufficient insurance to cover risks and associated liabilities arising from its operations and activities, consistent with contractual requirements. When outsourcing or subcontracting services, activities or functions, or operations, the organization should ensure the subcontracted or outsourced entity has appropriate insurance cover for those activities.

The organization should provide documentary evidence that they hold current and paid up to date insurance as appropriate and relevant to the contract in the proposed areas of operations, as follows:

a) general liability insurance for third party claims of bodily injury or property damage;

b) professional liability insurance for negligent acts arising from professional loss, bodily injury or property damage;

c) employers liability (including maritime employers liability). The organization should establish with the client and underwriters the need to review all provisions in their own property and liability insurance policies to cover the deployment of a PCASP and firearms aboard;

d) workers compensation as applicable;

e) personal accident insurance (tropical disease, accidental death, temporary or permanent disability) with medical and evacuation expenses; and

f) any other coverage as indicated by the risk assessment.

As firearms and other security related equipment are to be part of the contracted plan, the organization should insure their personnel to carry and use firearms on such voyages for accident, injury and damage arising from the use of firearms, and for liability that might arise from the carriage and/or intentional use or negligent misuse of firearms.

The organization may also consider other liabilities.

4.2 Planning

4.2.1 Security management policy

The organization should operate a security management system such as ISO 28000 or similar.

The organization should establish and be able to demonstrate ongoing evaluation of its compliance with the security management system and the need for continual improvement.

Top management should define and document:

a) the organization’s commitment to a security management policy;

b) the organization’s ability to provide services to meet client needs in conformity with applicable and relevant international and national law and regulatory requirements;

c) its commitment to a risk management approach to business planning.

The security management policy should also:

1) be available to all interested parties and stakeholders;

2) allow a client reasonable scope to perform due diligence for the management of the services retained;

3) be communicated publicly so all interested parties and stakeholders have easy access to it within the organization;

4) comply with applicable and relevant international and national laws, codes and regulatory requirements.

4.2.2 Actions to address risks and opportunities

The organization should consider risk criteria that may impact its operations as follows:

a) identify predictable risks which can impact on the activities, business and reputation of the business or those of interested parties and stakeholders;

b) systematically evaluate and prioritize risk controls, management, mitigation and treatments and their cost effectiveness;

c) be kept under review and regularly updated in light of the context of operations of the organization;

d) continually evaluate the effectiveness of risk treatment options post incident and after training or exercises;

e) ensure that the risk assessment is taken into account in carrying through the security management system;

f) identify applicable risk requirements for any subcontracted entities.

The organization should also formally record its objectives and targets for the management of risk by preventing and deterring threats. This should include commitments to:

1) minimize risk by adequate preparation and resilience;

2) provision of security for employees and contracted or sub contracted personnel and as set out in a contract and under the authority of the Master for crew and passengers against external threats;

3) comply with legal and other regulatory requirements;

4) protect tangible and intangible assets as provided for in a contract;

5) continued improvement.

4.2.3 Security objectives and plans to achieve them

The organization should establish security objectives at relevant functions and levels, with the aim of managing risk by reducing the probability of events, minimising the effects of incidents and mitigating the consequences by adequate preparation and resilience. Legal and regulatory requirements should be identified and incorporated into the security objectives.

The security objectives should:

a) be consistent with the security management policy;

b) be measurable (wherever practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated; and

f) be updated as appropriate.

The organization should retain documented information on the security objectives.

When planning how to achieve its security objectives, the organization should determine:

1) what will be done;

2) what resources will be required;

3) what jurisdictions will be covered;

4) who will be responsible;

5) when it will be completed;

6) how the results will be evaluated.

4.2.4 Legal, statutory and other regulatory requirements

The organization should identify and incorporate into the security management system all legal and regulatory requirements, as well as any applicable Codes and Conventions. These should form part of contract negotiations with a client to take account of differing jurisdictions and statutory requirements as between home, flag, coastal and port states. An example of a frequently used commercial contract is listed in the Bibliography.

The organization should establish, implement and maintain procedures to:

a) identify applicable and relevant international and national legal, regulatory and other requirements related to its activities and those of any subcontractors, functions, clients, contracts and areas of operations;

b) identify relevant and applicable international and national laws and agreements which include but are not limited to the:

   1) applicable and relevant requirements of UNCLOS and maritime law;

   2) laws and regulations of the home states and flag and coastal states, recognizing that any decision whether to allow a PCASP aboard is the prerogative of the flag state;

   NOTE Article 92 of UNCLOS refers to the flag state's exclusive jurisdiction on the high seas and article 94 refers to "duties of the flag state".

   3) applicable national laws relating to the procurement, carriage including export and import licensing, storage, use and disposal of firearms and security related equipment;

   4) conventions and laws relating to bribery, corruption and graft;

   5) employment law and human rights obligations and any other commitments to which the organization may subscribe.

The organization should ensure that its procedures provide for the following and consider how these requirements apply to its operations, including the availability of specialist maritime legal advice on a 24 h basis, and in particular:

a) appropriate prior approval from the flag state and compliance with any home state regulations, as regards the deployment of PCASP;

b) appropriate prior approval and any licence necessary for the carriage, transit and brokering of firearms and other controlled goods ;

c) appropriate prior approval as regards the deployment of PCASP from countries in which operations are conducted or managed, or countries through which PCASP may transit;

d) appropriate prior approval and licences for the transport, carriage, storage of firearms and security related equipment from, into or through a state;

e) specific prior approval and licence for the storage of firearms and security related equipment from the flag state aboard for any period longer than a single transit.

The organization should record this information and keep it up to date. Relevant information on legal and regulatory requirements should be communicated to persons working on its behalf and who are part of the supply chain and/or subcontracted.

4.2.5 Authorization and licensing of firearms and security related equipment

The organization should establish and document its processes for compliance with home state, coastal and flag state laws as regards the procurement, licensing and transhipment of firearms for each transit. Processes should also be established and documented for the licensing of individuals to use such firearms in the areas of operations where this is required under home, flag state or coastal national state (e.g. port, transit) laws. These processes should include a detailed plan of this process for provision to the client.

The organization should:

a) acquire and maintain legal authorisations for the possession, export and transhipment of firearms and ammunition required by applicable national and international law;

b) ensure documentary evidence is available to prove that firearms are procured, transported, embarked and disembarked legally;

c) ensure that where firearms are to be transported across international boundaries, or where they are being held on board ship (in accordance with the laws of the relevant flag states), between coastal and port states they are in possession of all the required authorisations covering all elements of the operation;

d) have a central record of all firearms and ammunition held, by type, serial number and location detailing movement, issue, receipt, maintenance, modification, usage and disposal history;

e) have robust and legally compliant arrangements for the safe and secure storage and movement of firearms when not in use. This should include written agreements for storage ashore, with military, naval or law enforcement bodies of recognized state governments;

f) comply with any home or flag state or local requirements in respect of identifying and licensing individuals who will use such firearms, including “end user certificates” where national laws apply;

g) secure the necessary written authority from the flag state and where appropriate, the coastal state, for holding stocks of firearms and ammunition on the high seas or offshore.

The organization should also:

h) ensure that firearms issued to security teams are adequate for the task of deterring, and if necessary defending against Pirate Action Group attacks;

i) have detailed procedures for regular and frequent checks of firearms, ammunition and other security related equipment, and for investigating discrepancies;

j) ensure that firearms issued to PCASP are adequate for the contracted task, the risk assessment for the transit or operation being undertaken and are consistent with the terms of the commercial contract;

k) maintain records detailing the issuing and receipt of firearms, ammunition and equipment to personnel, showing the individuals to whom issued; serial numbers of firearms and equipment and the quantities and types of ammunition held;

l) have procedures to detail how ammunition is to be accounted for on deployed operations and reconciled on completion of a transit;

m) have procedures that cover arrangements for the safe testing and zeroing of firearms and any necessary permits for live firing exercises on board prior to undertaking assigned security tasks;

n) ensure that their personnel only use licensed firearms and ammunition as stipulated in the contract;

o) have procedures for the regular maintenance of firearms and security equipment to ensure they remain fit and safe for purpose;

p) establish and agree procedures with the Master as regards the designated areas aboard where firearms may or may not be carried, together with further agreed procedures about the state of firearms readiness;

q) establish and agree procedures with the Master as regards safe area loading and unloading of firearms and security related equipment.

4.3 Resources

4.3.1 General

The resources available should include information, management tools, human resources including people with relevant experience and specialist skills and knowledge, and financial support. In doing so, it should ensure that it is complying with applicable and relevant legal and regulatory requirements and meeting its designed objectives and targets.

4.3.2 Selection, background screening and vetting of security personnel, including PCASP

The organization should establish and maintain procedures for background screening and vetting of all security related persons working on its behalf to ensure they are fit and proper and qualified for the tasks they will carry out. Selection of qualified personnel should be based on specific competencies and criteria defined by the organization including knowledge, applicable and relevant military, law enforcement or equivalent experience, skills, abilities and attributes.

Background screening should be conducted in compliance with all relevant and applicable legal requirements. Where possible under individual privacy and data protection law, the screening should provide for:

a) consistency with both legal and contractual requirements;

b) identity, minimum age and personal history requirements;

c) review of employment history;

d) criminal background checks;

e) security and law enforcement service checks;

f) assessment of medical, physical and mental fitness of personnel (this may include psychometric testing and/or written evidence from a health professional);

g) history of drugs or alcohol abuse;

h) ongoing vetting to establish continued suitability for security operations in high risk areas which might involve the use of firearms;

i) assessment of fitness to carry firearms as part of assigned duties;

j) review of relevant experience and specific certification in the use of firearms to be deployed;

k) relevant documentation including for personnel deployed at sea such as a valid seafarer's medical certificate or national equivalent.

Other considerations:

1) minimum age requirements may be set by local, home or flag state law,including a commitment not to employ child labour as defined by ILO Conventions 182 (worst forms of child labour) and 138 (minimum age). In no circumstances should any person younger than 21 years of age be employed in duties that might require the use of a firearm;

2) records of the screening process should be maintained, where legally permissible, on personnel files under strict controls to keep them secure for at least seven years (or as required by local statute).

Contracts of employment should include a requirement for the individual to notify the organization of any circumstances that might lead to a review of their screening status and possible suspension of employment in accordance with applicable law.

4.3.3 Selection, background screening and vetting of sub-contractors

The organization is responsible for the work of any subcontractor and liable within applicable law for their conduct. All subcontracting should be agreed with the client in advance.

The organization should establish procedures for selection, background screening and vetting, including:

a) provide for appropriate written contractual agreements with the subcontractor;

b) advise the client of any such arrangement in writing and where appropriate, obtain client approval;

c) provide written evidence of the chain of authority from the organization to the subcontractor;

d) ensure that full insurance coverage is provided for the activities of the subcontractors;

e) the organisation's policies and those required by the standard, including health, safety and environment policies and procedures, and its Code of Ethics;

f) maintain a record of subcontractor conformance with the requirements of this International Standard.

4.4 Training and awareness

4.4.1 General

Persons doing work under the organization's control should be aware of the organization's security management policy and objectives, and the contribution they make to the effectiveness of that system and the benefits of improvement performance as well as the adverse implications of not conforming with the security system requirements.

4.4.2 Training standards

The organization should ensure that all persons performing tasks on its behalf, both including employees and, subcontractors, and outsource partners, have received adequate and appropriate individual and collective training to demonstrate competence in their allocated tasks and activities, to cover the full scope of the certification.

Records of that training should be available to demonstrate that the security personnel have the skills, knowledge and experience to undertake the assigned security tasks.

The organization should maintain comprehensive, detailed and auditable records of initial and refresher continuation training.

The organization should identify individual training needs associated with security management system training. The organization should establish, implement, and maintain procedures to ensure all security operatives performing tasks on its behalf are aware of and receive training in the following:

a) the roles and functions of security operatives as stipulated in the contract;

b) significant risks and current and potential threats that may be encountered in the area of operations;

c) applicable and relevant international and national legal and regulatory requirements;

d) procedures to reduce the likelihood and/or consequences of a disruptive or undesirable event, including procedures to respond to and report incidents;

e) the organization's policies and those required by the Standard, including health, safety and environment policies and procedures, and its Code of Ethics;

f) an absolute ban on bringing or consuming alcohol or illegal drugs aboard the ship at any time;

g) recognition of the strict limitations of their role at sea as set out in the contract, and the adverse implications of exceeding that defined role.

All training received should be in accordance with the requirements of the home and flag state laws, where applicable.

4.4.3 Training procedures and protocols

The organization should establish, implement, and maintain procedures to ensure all security operatives carrying out tasks on its behalf are aware of and receive training in the following:

a) familiarity with the maritime environment, including ship type and layout, navigation and communication methods, the roles of the crew as well as an understanding of capability and speed of the ship for the specific transit; the team leader should have verifiable familiarity of the ship type and the particular transit envisaged;

b) understanding of ship security systems and physical defence arrangements (e.g. ship hardening and use of citadels in accordance with best management practices);

c) a thorough understanding of the Rules for the Use of Force in general and as they apply for the specific transit being undertaken, in accordance with international law and the law of the flag state. This should include the command and control relationship between the PCASP and the Master, while recognizing the individual inherent right of self-defence;

d) knowledge of the operating environment including potential threats, and the role of relevant international, regional, and governmental or inter governmental organizations and entities;

e) relevant and applicable provisions of international and national law, and of SOLAS, International ship and Port Facility Security Code (ISPS), International Safety Management (ISM) and any current best management practice;

f) verifiable training that demonstrates competence with the specific firearms, ammunition and other related security equipment that will or may be used in undertaking their assigned duties;

g) familiarity with arrangements for storage, maintenance and inventory of firearms and ammunition;

h) the circumstances and authority under which stored firearms and ammunition may be removed from store and made ready for use, and the specific and clearly defined areas in which firearms may or may not be carried;

i) appropriate medical training including trauma to a recognized national or international standard with at least one of the security team designated as the Team Medic, having an appropriate first aid training qualification;

j) basic sea safety training appropriate to the ship type;

k) an absolute ban on bringing or consuming alcohol or illegal drugs aboard the ship at any time;

l) procedures to report on any incident and prevented incident or threat during the ship's transit;

m) training in dealing with any unauthorised persons aboard, including the progression from disarming an attacker and handing such a person over to the Master as an unauthorised person under the responsibility of the Master, not the PCASP;

n) procedures to log and report any incidents involving the use of arms, or any prevented incident which might require the use of force;

o) the organisation's policies and those required by the standard, including health, safety and environment policies and procedures, and its Code of Ethics;

p) communications protocols and procedures, including a clear chain of command and understanding of the role of the Master of the ship as the final arbiter;

q) their roles and responsibilities in achieving conformity with the requirements of the security management system;

r) the potential consequences of departure from specified procedures.

The organization should ensure that all personnel performing maritime security services receive not only initial but also recurring training on the security management system in general and as required for specific tasks.

4.4.4 Firearms training

To ensure the safe handling of firearms the organization should:

a) ensure that all personnel who are employed to carry and use firearms are trained and competent on the specific firearms they are intended to use and are assessed to be competent in their use prior to embarkation on board the ship and are updated on the applicable Rules for the Use of Force prior to deployment;

b) have systems in place to verify that personnel have been trained in the use of the specific firearms and other security associated equipment specified in the contract, and that they only use those firearms specified and for which they are qualified;

c) provide live fire training and evaluation for all personnel authorized to carry firearms and security related equipment in the performance of their duties. A documented level of competence should be demonstrated with the specific firearms authorized for use as specified by the organization, or to a higher level as required by law or contractual obligations. Those authorized to carry firearms should undergo refresher training at least once per year on the specific firearms authorized.

The organization should:

1) maintain training records for all personnel specifying what training they have received, and for which firearms they are considered qualified, signed by the individuals trained;

2) where personnel may need training on specialist equipment:

   i) ensure all personnel required to use specialist equipment are trained and familiar with it;

   ii) provide conversion and familiarisation training where appropriate;

   iii) maintain records of such specialist training.

4.4.5 Training records

The organization should establish and maintain records of training to demonstrate its conformity with the requirements of this International Standard.

4.5 Communication and awareness

4.5.1 Awareness

The organizations should ensure that personnel doing work under the organization's control should be aware of the organization security management policy, culture and Code of Ethics. The organization should also ensure that PCASP are familiar with:

a) the security objectives;

b) their roles and responsibilities in achieving conformity with the requirements of the security management system and security objectives, including the benefits of improved performance;

c) the implications of not conforming with the PMSC management system requirements.

4.5.2 Internal and external communication

The organization should determine the need for internal and external communications relevant to the PMSC management system including communicating throughout the organization the importance of:

a) meeting objectives under the security management system as set out in this International Standard;

b) meeting legal and regulatory requirements;

c) the implications of non-conformity with these requirements; and

d) the need for continual improvement.

The organization should establish, implement and maintain procedures for:

1) communicating with staff, whether employees or subcontracted personnel;

2) receiving, documenting and responding to communications from internal and external interested parties and stakeholders;

3) assuring means of communication during times of pressure and disruption with regular testing of communications for such circumstances;

4) clear policies and protocols for communicating with the media and internet-based networks with clear understanding as to lines of authority for such communications;

5) updating the Master on security information in advance of the transit [or, as an alternative: 'assignment being undertaken']. This can take either the form of a written briefing or a formal meeting.

4.6 Documented information and records

4.6.1 General

The organization's security management system, in addition to the requirements of ISO 28000, should include provision for creating and updating, controlling and preservation of documented information, security and security and integrity of data and information.

Record details of personnel's next of kin and written consent for contact to be made with them should the need arise, with established protocols as to how and by which suitably trained personnel this would be done.

4.6.2 Control of documented information

Documented information required by the security management system and by this International Standard should be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) adequate protection (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization should address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including preservation of legibility;

e) procedures and plans to ensure ongoing integrity of information, including regular data back-up and off-site or remote data storage;

f) a system for locating these assets, and detailed procedures for the control of and access to such documents;

g) documents from external sources relevant to the operation of the security management system should also be identified and controlled.

Records to be retained in keeping with applicable legislation and regulatory requirements include the following:

1) records required by this International Standard;

2) details of personnel screening subject to data protection rules;

3) human resources and training, including firearms training records;

4) process monitoring records;

5) inspection, maintenance and calibration records for firearms;

6) incident reports;

7) records of incident investigations and their outcome;

8) internal and external audit results;

9) management review results;

10) external communications decisions;

11) records of applicable and relevant legal and regulatory requirements in general, and for specific transits;

12) records of significant risk and impacts;

13) records of management systems meetings;

14) communication with interested parties and stakeholders;

15) end of transit report to be prepared by the team leader for the benefit of the client with full details of the security assignment, any operational matters, training and/ship hardening conducted and with recommendations as to any appropriate future security enhancements.

5 Operation

5.1 Operational planning and control

The organization should establish and document processes and protocols for legal authority and licensing, preparation, deployment, command and control and communication with its security personnel. The organization should be able to demonstrate that the processes and procedures are kept under review to remain current and are fully understood by personnel operating under its control, whether employees, or subcontracted personnel.

The organization should plan, implement and control the processes needed to meet operational requirements which should include the following:

a) established criteria for the processes including compliance with applicable and relevant legal and regulatory requirements, Codes, and standards including this International Standard;

b) implementing control of the processes in accordance with the criteria;

c) recording information to the extent necessary to have confidence that the processes have been carried out as planned;

d) detailed and documented standard operating procedures and protocols.

In particular, the organization should fulfil the following:

1) compliance with applicable national laws and regulations and Codes on the transport, carriage, storage, embarkation, disembarkation, or use of PCSAP and firearms and security-related equipment on a case by case basis;

2) a demonstrable ability to manage risk;

3) a clear understanding of the operational environment and the changeable nature of the threat;

4) demonstrate the capacity to cope with unexpected developments and disruption which might require a response outside standard protocols and actions to mitigate any potential adverse effects in order to ensure the safety and security of the client's personnel and property and the personnel of the PCASP;

5) such incident management scenarios should be tested at least annually and records of such exercises kept and documented in order to:

   i) ensure that outsourced processes are controlled and consistent with established criteria and this International Standard;

   ii) demonstrate and document that these are understood by all its security personnel, whether employed or subcontracted;

   iii) provide guidance to security personnel on responses if any of their personnel are injured, killed or kidnapped, distinguishing between the role of the Team Leader and the role of the Master.

5.2 Command and control of security personnel including security team, size, composition and equipment

5.2.1 Command and control

The organization should establish that the command arrangements (and associated responsibilities) between the ship-owner/operator, Master, ship's officers and security team leader and other security personnel have been clearly defined and documented (such as an organigram or responsibility flow chart) with the client before embarkation. In addition, the organization should establish with the client that the Master and crew will be fully briefed about the security personnel's role on board, their responsibilities and concept of operations.

The command and control structure should provide for:

a) recognition that at all times the Master remains in command and is the overriding authority on board, and a progression in authority should the Master be unavailable or incapacitated;

b) documented ship and voyage specific governance procedures, inter alia, covering procedures for the conduct of exercises and real incidents;

c) specified duties and expected conduct of personnel on board including an absolute ban on the consumption of alcohol and drugs; and

d) transparent two-way information flow and effective coordination and cooperation between the ship-owner, organization and the ship's Master, officers and crew.

The organization should also:

— provide the team with communication equipment for internal communication between team members when embarked and training in its use. The equipment should comply with the safety requirements for the ship or platform and be fit for purposes of maritime operations;

— establish and document procedures for briefing the Master in advance of the transit being undertaken.

5.2.2 Size and composition of security team

The organization should demonstrate that the size and composition of the security team and the equipment they deploy has been discussed and agreed with the client. These agreements should be recorded in writing as part of the contract. Any requirements of the flag or home state should be respected in the contracting arrangements. In the contractual agreement any existing requirements of the flag State or home state have to be respected.

Elements affecting this decision may include:

a) length, breadth and size (gt) of the ship, speed, freeboard, and duration of the transit;

b) latest threat assessment and other intelligence;

c) agreed duties of the team;

d) the necessary licences and export/import and transit permits for firearms and security personnel permitted to use them;

e) specialist skills required;

f) anticipated embarkation and disembarkation port and dates with any additional ports being visited during the transit.

Where it is identified that the number of security personnel plus crew will exceed the existing number of people specified on the ships safety certificate, or similar, then procedures are needed to agree with the client to arrange the additional requirements as necessary with the flag state for temporary increase in provision as applicable.

Ensure that for the safety and security of ship's crew and passengers, the security personnel should at all times use uniforms and markings to identify their role as private security personnel; such identification should be distinguishable from all others on board the ship.

5.3 Guidance on Rules for the Use of Force (RUF)

The organization should agree with the client and the Master in advance defined and documented procedures for the Use of Force in accordance with international and flag state law, which should be annexed to the contract.

The organization should have a detailed and documented response plan which provides for:

a) reasonable steps to avoid and deter the use of force;

b) a graduated deterrent approach to protect personnel and assets in accordance with the contract. These should be reasonable and necessary including non lethal options and warning shots;

c) use of force reasonable and necessary to deter threats and appropriate to the situation consistent with applicable law. The plan should reflect that it is the team leader who should advise the master that it is necessary to invoke the Rules for the Use of Force;

d) a Use of Force continuum to resolve threats with minimum necessary force, recognizing that the response may move from one part of the continuum to another in a matter of seconds;

e) guidance on the Use of Force shall reflect that any use of lethal force can only happen in self defence and defence of others if there is an imminent threat of death or serious bodily harm , and should be reasonable and necessary to deter the threat;

f) the role and authority of the Master of the ship and that his decisions will be binding, without derogating from the inherent right of self-defence. The plan should reflect that if the Master judges that there is a risk to the safety of the ship, crew and or environment, he has the authority to order the security personnel to cease firing;

g) a written report of details of any attack or use of force to appropriate international liaison and to the authorities of the flag state, as well as to client and insurers;

h) where possible and practicable, a visual (and audio) record of any attack.

Where the Master is not available then the above role refers to the senior officer in command on the ship.

5.4 Incident management and emergency response

The organization should establish and carry out incident management procedures to identify threats and potentially harmful and disruptive events which could impact on the organization, its activities, services, interested parties and stakeholders and the operational environment. The procedures should document how the organization would prevent, mitigate and respond to events.

In doing so, the organization should consider each of the following actions, under the authority of the Master:

a) the safeguarding of life and promoting safety of personnel;

b) prevention of further escalation of the threat or a potentially harmful or dangerous incident;

c) minimising disruption to operations;

d) notification to appropriate authorities and international liaison;

e) protection of the image and reputation of the organization and its client;

f) corrective and preventative actions to avoid a recurrence.