EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT
Directorate A - Policy coordination
A.5 - Security

European Maritime Safety Agency

MARSEC Doc. 8708 annex

Interim Guidance on Maritime Security for Member States' Competent Authorities

Version. 2022

DISCLAIMER

This document has been developed by the European Commission with the assistance of the European Maritime Safety Agency with a view to providing to EU Member States' Maritime Administrations/Designated Authorities guidance in the application of maritime security measures.

The document does not have a regulatory purpose. None of its content is binding in nature or should be interpreted as superseding any legal/regulatory framework governing the implementation of maritime security in the Member States, be it national, European or international, more particularly the maritime security requirements of Regulation (EC) No. 725/2004 and of Directive 2005/65/EC.

This document is not a manual covering all aspects of security in the Regulation and the Directive. The selected content in this document is intended to specifically address areas for improvement identified notably during European Commission inspections in Member States; the content is intrinsically non-exhaustive, based on observation during activity carried out until the time of writing. It therefore does not preclude the correctness of possible other practices not considered or adequately reflected herein.

This is a living document that will be revisited within the MARSEC Committee at least on a yearly basis at the initiative of the Commission and notably based on the observations during Commission inspections in Member States

The guidance in this document should always be considered subject to and in conjunction with reference to the Member States' specific regulatory and operational contexts and any other relevant circumstances

The content of this document is not restricted but it is intended for the use of all personnel responsible for security in the EU maritime sector. Therefore, the dissemination of the content is not limited but encouraged. In this regard, national administrations are advised to share this document with those in the private sector that might benefit from it (i.e., Port Facility Security Officers, Company Security Officers, etc).

Table of Contents

List of Acronyms

AIS	Automatic Identification System
ASA	Alternative Security Agreement
CoP	Certificate of Proficiency issued in accordance with the STCW Convention and Code
CSR	Continuous Synopsis Record
DAO	Duly Authorised Officer
DoS	Declaration of Security
ESA	Equivalent Security Arrangement
EU	European Union
FSI	Flag State Inspector
ILO	International Labour Organisation
IMO	International Maritime Organisation
ISM	International Safe Management Code
ISPS	International Ship and Port Facility Security Code
ISSC	International Ship Security Certificate
IISSC	Interim International Ship Security Certificate
LRIT	Long Range Identification and Tracking of Ships
MLC	Maritime Labour Convention
MarSec	Maritime Security Committee
PDoS	Permanent Declaration of Security
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PSA	Port Security Assessment
PSC	Port State Control
PSO	Port Security Officer
PSCO	Port State Control Officer
PSP	Port Security Plan
RSO	Recognised Security Organisation
SOLAS	International Convention for the Safety of Life at Sea, 1974, as amended
SSA	Ship Security Assessment
SSAS	Ship Security Alert System
SSO	Ship Security Officer
SSP	Ship Security Plan

1. Introduction

1.1. Goals and purpose

This document provides guidance to assist Member States in achieving a harmonised and effective implementation of Union law in the field of maritime security, particularly Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security (hereinafter referred to as the Regulation) and Directive 2005/65/EC of 26 October 2005 on enhancing port security (hereinafter referred to as the Directive).

In particular, this guidance focuses on administrative and control tasks that need to be executed by Member States' Competent Authorities for maritime security in relation to the following areas:

- Member State obligations;
- Role as flag State;
- Role of Recognised Security Organisations (RSOs);
- Role as port State (i.e. Duly Authorised Officers, DAO);
- Port Facilities;
- Communication of information.

It should be noted that this document is not intended as a manual for ship and port / port facility security. It does not address every single aspect of this activity; such aspects are already covered by a vast array of literature published by various industry stakeholders. Instead, the added value of the document is to provide guidance on **selected** aspects of this activity where the feed-back from maritime security inspections led by the European Commission in Member States with the assistance of EMSA allows to highlight key regulatory requirements, providing more clarity where possible, together with recommendations and best management practices as a complement to the said requirements. In this, the guidance recalls considerations and interpretations agreed within the MARSEC Committee and takes into account IMO instruments as relevant. Member States are recommended to refer to these documents as necessary. Moreover, since the work of all parties involved in maritime security in Member States and the work of the European Commission inspectors are a continuous progress, the outcomes showed in this document should be in continuous development. Therefore, this is a living document that will be updated and developed as needed and at least on a yearly basis.

1.2. Scope

The scope of this guidance is related to the implementation of the EU legislative framework and applies to:

- All ports falling into the scope of the Directive;
- All ships and port facilities falling under the scope of SOLAS XI-2:
- With respect to domestic shipping all ships falling under Art. 3 para. 2 and 3 of the Regulation. These are:
  - Class A passenger ships within the meaning of Article 4 of Directive 2009/45/EC of 6 May 2009 as amended on safety rules and standards for passenger ships operating domestic services and to their companies, as defined in SOLAS IX-1, and to the port facilities serving them;

  - Different categories of ships operating domestic services, their companies and the port facilities serving them, in their application of the Regulation as determined by the Member State in question pursuant to mandatory security risk assessment required by the said Regulation.

Definitions used in this guidance are those referred to in Regulation 1, Annex I of Regulation (EC) 725/2004 of 31 March 2004, Article 2 of Directive 2005/65/EC of 26 October 2005 and Article 2 of Commission Regulation (EC) 324/2008 of 6 April 2008. Unless otherwise specified herein, any reference in this document to “articles” shall be in respect of articles of the Regulation and the Directive.

1.3. List of Symbols

🧭 Highlighting of key practices/obligations set by legislation. The **importance to recall** these elements arises from aspects where, in the course of European Commission MarSec inspections, margins for improvement in implementation have been identified.

👍 **Recommendations** applied by one or more Member States which have a potential added value in the effective implementation of the legal requirements.

✓ In addition, identified **best practices** are highlighted in text boxes along the document.

2. Applicable Union Law

The Regulation not only provides a basis for the harmonised interpretation and implementation of SOLAS XI-2 and the ISPS Code but also makes mandatory some of the recommendations of Part B of the Code. The main focus is to provide a standardised, consistent framework for:

- Establishing the respective roles and responsibilities of the various parties involved;
- Evaluating risk and enabling governments to make changes to security levels based on the vulnerability of ships and port facilities;
- Ensuring that adequate and proportionate maritime security measures are in place. In this context, the Regulation (Annex I Part A section 1.3) includes functional requirements aimed at inter alia:
  - Establishing a framework involving co-operation between the various parties;
  - Ensuring the collection and exchange of security-related information;
  - Providing a methodology for security assessments.

The Code’s regulatory approach to security implementation is two-pronged; on top of the risk-based approach reflected in Ship Security Assessments (SSAs) and Port Facility Security Assessments (PFSAs), the Code also applies a prescriptive approach, with a set of minimum requirements to demonstrate compliance.

Although the Code is self-contained, it cannot be taken in isolation from other maritime legislation that serves maritime security purposes. When dealing with security, it is necessary to consider the relevance of and relationship with other SOLAS regulatory aspects such as LRIT (SOLAS V/19-1) and AIS (SOLAS V/19) (in terms of links to security equipment), minimum safe manning (SOLAS V/14) (as may be relevant in the context of the implementation of the SSP (Ship Security Plan)), ISM (SOLAS Chapter IX), IMO number (SOLAS XI-1/3 and 3-1), the CSR (Continuous Synopsis Record, SOLAS XI-1/5), seafarer training (STCW Convention and STCW Code), the SUA Convention (suppression of unlawful acts at sea) and other non-IMO Conventions such as ILO 180 and/or MLC 2006.

The Directive aims to extend security measures more widely to areas of port activity. It covers the port as a whole, including the water surface, critical objects which are not port facilities but in the port and calls to re-examine port facility security plans taking into account the neighbourhood of any port facilities.

It has the same systemic approach as the Regulation: based on a port security assessment, a port security plan has to be developed; the Directive addresses also training, exercises and drills.

2.1. Member State obligations in relation to the Regulation 725/2004 and Directive 2005/65/EC

The Regulation and the Directive attribute to Member States two key categories of tasks – Administrative and Control – that, when properly addressed, should lead to their satisfactory implementation. For the proper fulfilment of these obligations Member States shall designate roles to their various relevant organs, develop a national programme and properly assess risk. Member States shall also ensure that port security measures introduced by the Directive are closely coordinated with measures taken pursuant to the Regulation.

2.1.1. Assignment of responsibilities within the Member State

In relation to the assignment of responsibilities Member States have a critical role. A Member State acting as flag State needs to address the processes of monitoring, controlling and verifying compliance by its own fleet while, as port State it is in charge of the control of ships calling or intending to call at its ports while, through a Designated Authority, it is also responsible to implement the legislation in port facilities. All this may be carried out by different organs within the different services, should they be local, regional or national, and some activities may be delegated to RSOs, hence involving multiple entities. Member States shall designate a port security authority/ies - responsible for the preparation and implementation of port security plans based on the findings of port security assessments - for each port covered by the Directive.

In setting up these functions and roles, it is **important** to ensure:

- Sufficient human and technical resources are devoted, with an adequate level of expertise to be able to interpret, administer and enforce legislation in a consistent manner;
- Clarity is established on how competent authorities conduct maritime security-related functions in line with the Regulation and the Directive;
- Cooperation is effective between relevant national bodies to assess the risks in ships and port facilities;
- That a mechanism is in place whereby intelligence data is available to Maritime Administrations and/or Designated Authorities to enable them to determine the appropriate Security Levels and that a system of Security Levels for ports or parts of ports is introduced for the purpose of the Directive.

In this regard it is **recommended** that the Member State establishes clear processes for the:

- Appointment of government officials to provide advice or assistance to ships (flying their flag or entering their waters) and to whom those ships report security concerns;
- Designation of the competent authority to receive SSAS messages;
- Appointment of a recipient of maritime security-related communications from other Contracting Governments;
- Implementation, update and revision of any relevant legislation and policies adopted. The following are examples of decisions in this respect, that have an impact on the national requirements for maritime security:
  - The extent of application of SOLAS XI-2 and the relevant sections of Part A of the ISPS Code to those port facilities within the Member State’s territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving from or departing on an international voyage;
    - Types of criteria may be established by the Member State at the national level to identify the port facilities to be considered as occasional in the context of the ISPS Code, for example setting a maximum number of calls per year or a pick of seasonal activity, or identifying particular features or types of vessels or activity (e.g. only used as a disengagement pier, no loading/unloading facilities, waiting berth, etc.); ESAs may often be appropriate for such port facilities;
  - Conclusion of Alternative Security Agreements (ASA) with other SOLAS Contracting Governments covering short international voyages on fixed routes between port facilities located within their territories;
  - Allowing ships entitled to fly its flag to implement other security measures equivalent to those prescribed in SOLAS XI-2 or Part A of the ISPS Code;
  - Allowing port facilities, other than those covered by an ASA, to implement security arrangements equivalent to those prescribed in SOLAS XI-2 or Part A of the ISPS Code;
  - In relation to control and compliance measures, determination of issues such as: necessary qualifications and training of DAOs, ships intending to enter a port of another contracting government or control of ships in port,

  - When carrying out monitoring activities, the role of the Administration reflected by extension in the roles of its officers. In the case where more than one authority is involved, suitable cooperation is necessary the modalities of which must be clearly established.
- The conduct of port security assessments that effectively take into account as a minimum the detailed requirements laid down in Annex I of the Directive[1].
- The drafting and adoption of port security plans that effectively take into account as a minimum the detailed requirements specified in Annex II of the Directive[2].

2.1.2. National Programme

National programmes for the implementation of the Regulation[3] are instruments in which Member States describe their overall systems for maritime security, covering both ships and port facilities, including the responsibilities of the various national, regional and local authorities involved in said implementation.

👍 It is **recommended** that Member States take into account the following when developing, reviewing and updating their national programmes, as indicated in Recital 14 and Article 9(1) of the Regulation:

- The responsibilities, principles, criteria, procedures and delegation of authority, as indicated in the guidelines and instruments from the IMO, such as *"Guidance on voluntary self-assessment by SOLAS Contracting Governments and port facilities"* (MSC.1/Circ. 1192) and *"Guidance on voluntary self-assessment by Administrations and for ship security"* (MSC.1/Circ. 1193);
- Changes to international and EU law in the maritime field that may have an impact, considering not only maritime security legislation;
- Potential need for their review every time there are structural changes to the responsible bodies in the Member State, amendments to National or Union law or other changes in related national strategies or approaches;
- Periodical revision at least every 5 years;
- That a National Maritime Security Committee is set up to bring the different organisations and stakeholders involved together to coordinate their activities and to provide advice on security issues taking into account the different responsibilities of the organisations with tasks under the programme;
- National programme also includes the aspects linked to the implementation of Directive 2005/65/EC

[1] Article 6, Dir.2005/65/EC
[2] Article 7, Dir.2005/65/EC
[3] Regulation Art. 9.3

2.1.3. Member States Risk Assessment

The EU regulatory framework previously presented outlines a standardised and consistent framework for:

- Evaluating risk;
- Enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities;
- Taking security countermeasures for ships and port facilities.

The assessment of risk is conducted at two levels:

- At a first level, Member States need to consider the threat to national maritime-related assets both locally and globally and any risk of attack thereto. Information to this effect will help Member States to decide on the basic security measures that should be applied at Security Levels 1, 2 and 3, and the circumstances in which the different Security Levels should be activated for both ships and port facilities;
- At a second level, the specific competent authorities for ship security and port facility security are encouraged to develop guidance/policies for the maritime sector – including companies responsible for ships flying the Member States' flag and RSOs designated to carry out tasks on its behalf – to be taken into account when:
  - Carrying out SSAs and PFSAs; and
  - Defining the specific security measures to be mandated in the SSPs and PFSPs.

It is **recommended** that:

- The risk assessment mechanism requires the interaction between the competent authority and industry, being the exchange of information particularly important in this collaboration. In this respect, reliable intelligence and quick dissemination of information should be as wide as possible to the shipping cluster;
- The policy guidance is reviewed on a regular basis, or at least every 5 years, to ensure that the assessments and plans are up-to-date, and these reviews are linked to the conducting of meaningful risk assessment for ships operating in domestic services as defined in Article 3(3). In this latter respect, instruments such as IMOs "*Guidelines on security aspects of the operation of vessels which do not fall within the scope of SOLAS XI-2 and the ISPS code*" (MSC.1/Circ.1283) may be useful as a reference.

2.2. Setting Security level and providing guidance for protection from security incidents

Member States are required[4] to:

- Set the security level (1, 2 or 3)[5] applying to ships or port facilities, taking account of general and specific threat information;
- Provide updated security level information that matches current security threats.

[4] Reg. 725/2004/ Annex I Reg.3 and 7. And Annex III Part B/4.8

In relation to the security levels of port facilities, it is **important** to recall that:

- Prior to entering and during a call at a port facility, ships must comply with the requirements for the security level set by the port Member State, if the security level is higher than that of the ship. In this case the port Member State must ensure that security level information is conveyed to ships operating in – or having communicated their intention to enter – its territorial sea.

It is **recommended**[6] that:

- Information on the change of security levels is sent to the ship via the CSO[7];
- MS should encourage Companies to use a cascade system whereby information that fails to directly reach the CSO is disseminated to all ships of the company;
- When multiple Member States are involved – e.g. in case of fixed routes between Member States, or in case of ships flagged in the EU operating in different parts of the world – there is good coordination between the Member States in setting the applicable security level, notably including exchange of information about changes in security levels they have set;
- Member States apply, at each security level, similar standards of security. This requires a degree of agreement and co-ordination between said States.

3. Bilateral or multilateral arrangements

3.1. Alternative Security Agreements vs Equivalent Security Arrangements

ASAs[8] and ESAs[9] can be distinguished by the following factors:

- ASAs are bilateral/multilateral security agreements applied to short international voyages on fixed routes located in the territories of the two/or more States, which are intended to deliver at least an equivalent level of security;
- ESAs can be adopted in respect of ships or port facilities, individually or in group. The effectiveness of such security measures needs to be guaranteed provided such security arrangements are at least as effective as those prescribed in Chapter XI-2 of the SOLAS Convention and the relevant mandatory provisions of the ISPS Code;
- Ships or port facilities covered by an ASA cannot also be subject to an ESA.

It is **important** to recall that:

- The agreements are to be notified[10] to the Commission which has four months to carry out the analysis to determine whether or not such agreements guarantee an adequate level of protection;

[6] MARSEC Doc. 0206 and MARSEC Doc. 0302

[8] Reg. 725/2004/ Article 5, Annex I Regulation 11 and Annex III 4.26
[9] Reg. 725/2004/ Article 5.4, Annex I Regulation 12 and Annex III 4.27
[10] Reg. 725/2004 art.5.2

- The MARSEC Committee has established a set of principles[11] that should apply to fixed routes; these principles include the proposal for ships and port facilities on such fixed routes to be covered by an ASA;
- ASAs need to be reviewed at least every five years[12];
- For ships, issues such as key shipboard operations[13] should be addressed in the ASAs;
- ESAs[14] may allow under duly justified circumstances Port Facilities to carry out ISPS activity without having to bear the full administrative, financial and organisational burden of a fully ISPS certified facility;
- Prior to allowing a ESA, a PFSA must be conducted and approved. The decision between implementing an ESA and a PFSP must in all cases be based on the conclusions of an approved PFSA. This conclusion should clearly state that an ESA can be implemented instead of a PFSP[15].
- MSs can either establish generic criteria defining the circumstances under which ESA may be adopted, or whether they use a case-by-case approach[16].
- An ESA must at least describe the security measures set out in the ISPS Code Part A, Section 14.2, and any additional security measures a MS deems appropriate or has rendered mandatory, and they must be at least as effective as the same measures when described in a PFSP[17];
- ASAs and ESAs are also subject to Commission inspections.

It is **recommended** that:

- Laid up vessels are not subject to ESA.
- MSs clearly define the criteria to authoise the adoption of an ESA, particularly the concept of occasional ISPS activity. In this regard, please see section 2.1.1.

It is a **good practice** that

- The use of an ESA instead of a PFSP may be considered as a practical solution in certain situations where a Port Facility:
  - Has been recently built and requires the immediate start of operations before the drafting and approval of a PFSP;
  - Is undergoing construction works or perimeter modifications that make the updating and re-approval of the PFSP more difficult during a certain period of time, until the situation has stabilised.

[11] MARSEC 1705 on Updated Guidelines on Alternative Security Agreements
[12] Reg. 725/2004 art.5.3
[13] Reg. 725/2004 Annex III Part B 4.26
[14] MARSEC Doc 7608
[15] Reg. 725/2004 Annex II part A 15.7
[16] MARSEC Doc 7608
[17] Reg. 725/2004 art.5.4

3.2. Declaration of Security

Declarations of Security (DoS) are requested by a party (ship or port facility) in order to specify what measures are to be taken during the ship/port interface or ship-to-ship activities to ensure adequate security of ships and port facilities notably when normal conditions of operation do not apply (e.g. when a ship and port facility are not at the same Security Level). The circumstances under which a DoS may be required should be determined by the Member State based on a risk assessment[18].

There are situations where a so-called `Permanent Declaration of Security´ (PDoS) is established. In these situations, its duration and the circumstances when it becomes invalid need to be carefully defined by the relevant national authorities following security assessments of the interfaces or activities involved.

It is **important** to recall that:

- Member States should inform companies of ships flying their flag as to the circumstances when a DoS needs to be requested by a Master/SSO of the said ships;
- Bunkering with non-ISPS certified ships outside an ISPS port facility is a ship-to-ship activity that warrants a DoS. When bunkering in a port facility, SSOs should liaise with Port Facility Security Officers (PFSOs) to establish whether the bunkering ships involved are certified before commencing operations;
- A PDoS could be agreed between a ship or ships of a company and a port facility where the ship calls regularly, to set out the respective security responsibilities. This can be especially useful in the case of Ro-Ro ships with short turnarounds in port;
- A DoS needs to:
  - Be signed by the ship and acknowledged by the port facility (when in a port facility)[19];
  - Include port facility LOCODE (when in a port facility) and record the port facility number;
  - Clearly indicate responsibilities, e.g. for carrying out security measures;
- Administrations must specify the minimum period for which DoS are to be kept on board by ships flying their flag.

It is **recommended** that:

- Requiring or responding to requests for a DoS is set out and clarified in the SSP in line with the regulation[20];
- PFSOs or any other party responsible for shoreside security be reminded of the need to acknowledge requests from ships for a DoS;

[18] Reg. 725/2004 Annex II Part A 5.1
[19] Reg. 725/2004 Annex II Part A 5.4
[20] Reg. 725/2004 Annex II Part A 5 and Annex III Part B 5

- A DoS is retained on board for as long as it relates to one of the last 10 calls at port facilities but, in any case, with a minimum recommended time of 3 years;
- Considering the current practice of SSOs requesting a DoS at every single port of call, even in cases not required by the SSP, Member States remind their shipping community that a DoS should not be the norm;
- When a PDoS is in place all shipboard personnel with security responsibilities should be made aware of the security measures taken by the port facility on behalf of the ship and vice versa. The same shall apply to port facility personnel with specific security responsibilities.

4. Enforcement and sanctions

As with most areas of maritime activity, the implementation of maritime security necessitates legislative and jurisdictional support.

It is **important** for Member States to:

- Ensure that their national legislation includes an enforcement regime accompanied by meaningful sanctions[21]. The legislation should also designate officials with clear authority to impose such sanctions;
- Recall that the imposition of security control and compliance measures in accordance with Reg. 725/2004 Annex I reg. 9 cannot be considered as a sanction.

It is **recommended** that:

- The authorities responsible for the enforcement of Article 14 of the Regulation clearly assign this activity to the officers in charge of exercising it;
- Irrespective of the ultimate sanctions available to a national authority, Member States take a stepped approach when seeking to ensure that a port facility or ship corrects an identified deficiency. In case there is a need for a more robust approach, that might warrant officers to take action in their capacity, said officers should act in an effective, proportionate and dissuasive way for which they need to be properly empowered and trained.

[21] Reg. 725/2004 art 14

5. Flag State

Member States who register ships under their flags effectively exercise their jurisdiction and control in administrative, technical and social matters over said ships as indicated in Article 94 of UNCLOS, in particular with regard to SOLAS and the ISPS Code.

It is **important** to recall that:

- Member States should establish an adequate and effective system for exercising control over ships entitled to fly their flag, and to ensure that they comply with relevant international rules and regulations in respect of, *inter alia*, maritime security.

It is **recommended** that:

- When a Member State approaches its flag State functions in respect of maritime security, it also takes into account other relevant legal instruments, namely the III Code (IMO Res. A.1070(28)) on the mandatory implementation of IMO instruments and Directive 2009/21/EC of 23 April 2009 on compliance with Flag State requirements.

It is a **good practice** that ✓

- quality systems based on the ISO 9000 series are introduced to improve the implementation of the Regulation.

The following sections provide guidance regarding Administrative tasks that fall within a Flag State's responsibility, followed by guidance regarding control tasks.

5.1. Manning level[22]

Generally, a number of crew members on board a ship is assigned necessary security tasks at different security levels as generally reflected in the process of setting a ship's manning level.

Difficulties can be encountered in situations where ships have a lower gross tonnage and therefore fewer crew members on board. In these cases, the additional work has an impact on daily tasks on board due to the need to implement security measures.

It is **important** to recall that:

- The additional workload resulting from the implementation of the Regulation needs to be taken into account when establishing the minimum safe manning of a ship;

[22] Reg. 725/2004 article 3.5 and Annex III Part B 4.28

- Ships need to demonstrate that they are able to implement the hours of rest on board (MLC 2006, ILO 180). Failure to do so constitutes non-compliance also with the Regulation.

It is **recommended** that:

- In determining the manning level for a ship, a Member State takes into account IMO Assembly Resolution A.1047(27), revising A.890(21) on *"Principles of Safe Manning"*. SOLAS Chapter V Regulation 14 recommends that a "Minimum Safe Manning Document" is issued;
- Particular attention is paid to ships with fewer crew members, where security could take up a significant amount of their workload.

5.2. Ship Security Assessment

SSAs are the first step in determining the security measures that should be implemented by ships. If they are not carried out effectively and with all the relevant information, the SSP drawn up based on the SSAs may not be effective either.

5.2.1. Content and approval

It is therefore very **important** that:

- SSAs consider all the potential threats and known security incidents, so that these can be addressed effectively in the subsequent SSPs. Some of the information necessary for this purpose will need to come from the flag State;
- The risk assessment is ship specific.

It is **recommended** that:

- Risk assessments are developed and reviewed taking into account the associated threats applicable specifically to that ship rather than simply cover threats of collective or generic applicability (e.g. to whole fleets or to a whole State);
- Member States issue guidance on identified potential threats that ships may face (e.g. piracy, cyberattacks), both at sea or in ports in different parts of the world where they might be operating. This guidance should be updated on a regular basis. Where a company has ships flying different flags, this guidance should be sought from each flag State as the threats may be different;
- When cyber risk management is considered within the ISM (IMO Resolution MSC.428(98)) specific reference should be mentioned both in the SSA and in the SSP, to fulfil the Regulation[23]. On the other hand, if cyber risk management is considered within the SSA and SSP, or in an independent Cybersecurity Plan, specific reference

[23] Regulation 725/2004, Art. 3.5 and Annex III, Part B section 8.3

could be mentioned in the Safety Management System of the ISM to comply with the mentioned resolution;

- If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included;
- Attention to potential confidentiality issues when cyber risk management is considered within the ISM (IMO resolution MSC.428(98)).

It is a **good practice** ✓

- Conducting a specific cybersecurity vulnerability assessment as an enhancement to the generic SSA;
- Introducing the design of cyber resilience architecture in the design of the new building networks.

5.2.2. Reviews and amendments to a SSA

👍 It is **recommended** that:

- SSAs (and subsequent SSPs) be updated regularly to take account of ever emerging threats, current examples being cybersecurity and remotely piloted aircraft systems. However, this should not mean that a review should necessarily lead to change in the SSA, but that different potential scenarios were considered and that resultant conclusions were documented;
- SSAs are reviewed when there are changes in circumstances such as the ship's operating area or equipment, or if problems are identified during operations, training, drills, or following a security incident;
- Records of the review process be maintained.

5.3. Piracy

It is a **good practice** that ✓

- When a Member State approaches its flag State functions in respect of maritime security, it should build and operate networks with the maritime industry as well as with international partners to exchange necessary information and practises to defend piracy at sea (e.g. The German Federal Police has been operating a piracy prevention centre (PPC) since 2010 and acts as an interface between the maritime industry, national and international authorities.).

5.4. Ship Security Plan

5.4.1. Content and approval

When approving an SSP, it is **important** that the Administration:

- Verifies that the SSP addresses all the applicable mandatory legal provisions on, *inter alia*, cargo handling, prevention of weapons or dangerous substances, procedures for auditing security activities, procedures for reporting security incidents (including cybersecurity incidents), maintenance requirements and frequency for the testing/calibration of equipment;
- Verifies that the SSP is consistent with the SSA in so far as ensuring that all the issues identified by the SSA are addressed through specific security measures in the SSP;
- Or the RSO acting on its behalf, has at its disposal the necessary expertise to enable it to approve the SSP;
- If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included.

It is **recommended** that:

- Measures are taken to guarantee the authenticity and integrity of the SSP on board. Among these measures might be the inclusion content tablet, index, and document control (e.g., include total number of pages in the page number, adequate record of changes). It should consider physical (e.g., safebox, locks,…) and digital (e.g., inclusion in the cybersecurity risk assessment,) aspects as required;
- Any amendments to an approved SSP, based on the verification carried out for that plan, shall be distinctly identifiable and do not replace the original plan;
- Approval of an SSP is indicated in such a way as to confirm that every page has been approved;
- A letter of approval of the SSP is issued and made available on board, which clearly identifies the SSP to which it refers;
- The SSP clearly indicates which parts cannot be made available to DAOs without prior consent from the Flag Administration, should said DAOs need access to the SSP in the event that clear grounds are established;
- Member States provide Masters and SSOs with clear instructions on making available the parts of the SSP that can be disclosed to DAOs in the event that clear grounds are established to this effect;
- Member States encourage companies to avoid unnecessary administrative burden by ensuring that SSPs are not excessively detailed and that they are tailored to apply to the specific ship and/or Company.

- When cyber risk management is considered within the ISM (IMO resolution MSC.428(98)) specific reference should be mentioned both in the SSA and in the SSP, to fulfil the Regulation[24].

5.4.2. Reviews and amendments to a SSP

It is **important** that Member States:

- Determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration[25];
- Ensure that when amendments to a SSP are approved, that approval date does not become the approval date of the SSP; the original approval date should be retained. A best practice consists of keeping a certified copy of said document with the SSP.

It is a **good practice** that ✓

- To include in the SSP an index, which can be used to show the validity date of each section, indicating where applicable when it was amended;
- That the plan allows proper traceability of amendments. With regards to this issue:
  - when amendments are made these need to be documented; and
  - if amendments have been made to the SSP, the index should identify these amendments, so that the SSO can easily trace the most recent;
- To ensure that there is a clear distinction between a new SSP – for which a verification must be conducted and a new International Ship Security Certificate (ISSC) issued – and an existing SSP duly amended as necessary.

5.4.3. Testing the effectiveness of the SSP

Approved SSPs are tested in accordance with Section A/4.4 of the ISPS Code[26]. This is intended to ensure the effectiveness of the approved SSP; it is not concerned with "*testing*" the implementation of the measures in the plan.

It is **important** to recall that:

- The Administration is to determine the extent to which it wants to carry out this mandatory activity;
- This task cannot be delegated;

[24] Regulation 725/2004, Art. 3.5 and Annex III, Part B section 8.3
[25] Reg. 725/2004 Annex II Part A 9.5 and MARSEC Doc. 2204 Rev.2
[26] Reg. 725/2004 Annex II Part A 4.4

- Member States may decide to carry out this activity in conjunction with other tasks.

👍 It is **recommended** that:

- Member States consider different ways of carrying out this testing activity.

5.5. Ship Security Officer

The Ship Security Officer (SSO)[27] is the person designated by the Company as responsible for the security of the ship and liaison with the Company Security Officer (CSO) and Port Facility Security Officer (PFSO).

🧭 It is **important** that:

- The SSO is duly trained in such functions and has the necessary authority on board to exercise her/his responsibilities under the general authority of the Master
- The SSO is fully conversant with the SSP and in particular, with his/her security duties (included cybersecurity duties, albeit considered within the ISM (IMO resolution MSC.428(98)) (i.e. obligation to report and maintain records of all security incidents). This needs to be confirmed during verifications.

👍 It is **recommended** that:

- Procedures are put in place to ensure that where regular crew changes occur, the new SSO on board is briefed by the outgoing SSO about any security issues as may have arisen;
- When cyber risk management is considered within the ISM (IMO resolution MSC.428(98)), the SSO should be fully aware of the cybersecurity measures indicated therein;
- The SSO's ability to carry out his/her security duties is not compromised by excessive workload related to other functions on board. In cases such as cruise operations for example, crew members with passenger interface responsibilities may not be able to act effectively in their role as SSO during a security incident.

5.6. Restricted Areas

Restricted areas (RAs) are intended to prevent access to persons who are not so authorised. These areas are identified during SSAs and designated as such in the related SSPs[28].

[27] Reg. 725/2004 Annex II Part A 12

[28] Reg. 725/2004 Annex II Part A 9.4.2

It is **important** to recall that:

- Whereas the legal obligation is for RAs to be so designated and for respective measures to be set up to prevent unauthorised access accordingly, particular attention should be given to ensure that, irrespective of how such areas are indicated in the SSP (whether through a drawing or a list, or both), the information given is consistent with the actual physical areas to which it relates;
- The measures approved in the SSP need to consider the daily operation of the ship in different ports of call with regards to the management of RAs;
- In the management of RAs, attention is to be paid to the compatibility of limiting access to or exit from such areas with the evacuation and escape routes that would be used for safety reasons (e.g. from the engine room).

It is **recommended** that:

- When RAs are identified in the General Arrangement Plan of the ship and included as annex to the SSP, the SSP describes the permanent or temporary measures for these areas;
- A clear distinction is made between the terms '*locked*' and '*closed*' given that these terms are often erroneously used interchangeably.

It is a **good practice** that ✓

- During the course of a verification or of a flag State inspection on board, Member States confirm that marking of RAs is consistent with what is indicated in the SSP.

5.7. Security equipment on board ships

The security of ships can be enhanced through the use of physical measures complementing procedures and personnel. The use of security equipment is considered as a part of the SSA; its use, maintenance, testing and calibration is specified in the SSP[29]. Such equipment should not be disactivated or replaced, or its use changed, without approval through an amendment to the SSP. Examples of security equipment that Member States may consider includes:

- Warning systems (e.g. audible and silent alarms);
- Card readers (e.g. to automated control of onboard access);
- Intrusion alarms (e.g. motion detectors, magnets, acoustic devices, infrared light);
- Active surveillance (e.g. CCTV);
- Locks (e.g. on doors to RAs);

[29] Reg. 725/2004 Annex II Part A 9.4.15 & 9.4.16

- Plastic seals (e.g. to quickly unlock access to survival crafts, fire stations, co2 rooms, etc. in case of an emergency;
- Substance and article detection (e.g. X-ray imaging);
- Network protection (firewalls, data storage protection).

It is **important** that:

- The security equipment described in the SSP corresponds to what is actually being used on board for security purposes;
- Crew members assigned with responsibilities for using such equipment are trained on and conversant in such use;
- Relevant procedures be included in the SSP.

It is **recommended** that:

- The Administration provides guidance as to how approval can be obtained for temporary equivalent measures adopted in the event of failure of security equipment provided that they will not compromise the security level of the ship. The administration should also consider how this approval is formally transmitted to the ship so that evidence can be adequately provided during inspections;
- If such equivalent measures are needed, an assessment is made by the CSO and approved by the Flag Administration to confirm that they are at least as effective as the security equipment they replace;
- Arrangements are made with security equipment suppliers to ensure that defective equipment can be repaired/replaced as quickly as possible, ideally at the ship's next port of call in cases where equipment breakdown happens while at sea;
- Member States and shipowners consider that temporary equivalent measures in the event of equipment failure should be agreed by the Administration to maintain the validity of the ship's ISSC[30].

It is a **good practice** ✓

- Consider the benefits of implementation of the most recent standards (e.g. IEC 61162-460, ISO 16425, IEC 62443) on board ships to improve cybersecurity.

[30] Reg. 725/2004 Annex II Part A 19.1.4 and Annex II Part B 9.6

5.7.1. Ship Security Alert System

The Ship Security Alert System (SSAS)[31] is an essential element for ensuring the security of a ship. It should be tested regularly, based on requirements to be laid down in the SSP[32], to ensure it is fully functional at all times.

It is **important** to recall that:

- During certificate verification, the SSAS must be tested and found in working order, with due care being taken to confirm that the installation is in accordance with the SSP;
- The frequency of tests of the SSAS must be specified in the SSP. Tests must be readily identifiable as such.

👍 It is **recommended** that:

- Member States develop procedures to notify other States in the vicinity of a ship which notifies a ship security alert;
- Member States' competent authority, designated by the Administration[33] as initial recipient of the security alerts from their flagged ships, should easily have access to General Arrangement Plans in order to facilitate the intervention of appropriate forces in case of need following a security incident.

5.8. Qualifications and Training

Training is necessary to understand the duties and responsibilities and to be able to properly perform security related tasks.

It is **important** to recall that:

- Since the adoption of the ISPS Code, mandatory requirements for the certification of seafarers in respect of their proficiency in security matters or in security awareness, have been introduced in the STCW Convention;
- Administrations must ensure that the documents to certify that seafarers have met the required standard of competence for maritime security in line with STCW (i.e. Certificates of Proficiency (CoP) and Security Awareness) are issued by authorised organisations.

👍 It is **recommended** that Administrations:

- Maintain a list of the organisations they have authorised and periodically assess their ability to exercise their tasks;

[31] Reg. 725/2004 Annex I Reg 6.
[32] Reg. 725/2004 Annex II Part A 9.4.18
[33] Reg. 725/2004 Annex I Reg 6.2.1

- Specify a maximum period of validity for CoPs;
- Require periodical refresher training for staff allocated security related tasks.

It is a **good practice** that ✓

- Cybersecurity training at different levels is considered as part of the security training programme in order to create a cybersecurity culture across the organisation.
- Introducing the figure of the Chief Information Security Officer (CISO) in the organisation to ensure that cybersecurity threats are considered, adequate preparedness measures are taken, and suitable response and recovery procedures can be implemented if necessary.

5.9. Drills and exercises

Security drills[34] are intended to be held periodically with the participation of crew members in order to establish that said crew members are alert and proficient and that the SSP is being implemented properly. Drills are operational and are designed for crew members to test and practice a specific procedure, task or routine related to their security role (e.g. baggage search, use of security equipment). Exercises, on the other hand, are organised on a larger scale intended to test the wider context of a security system including communication, coordination, availability, resources and reactions. Exercises are usually not limited to the ship but cover related parties like other ships flying the Member State's flag, shipping companies and authorities within the Administration responsible for maritime security.

It is **important** to recall that:

- Drills and exercises are carried out in order to maintain a high level of preparedness by in particular for those assigned security responsibilities;
- Member States should verify that the scope and conduct of drills and exercises correctly reflect the distinction between these two measures and their intended respective objectives;
- Drills should test one or more of the procedures in the SSP, covering one or more scenarios[35].

[34] Reg. 725/2004 Annex II Part A 13.4
[35] Reg. 725/2004 Annex III Part B 13.6

It is **recommended** that:

- The more frequently ships interface with port facilities, the more important it is that said interfaces are tested through exercises;
- When exercises are carried out, companies should provide feedback to their ships on any lessons learnt therefrom; the management of each such ship can then have an internal discussion about these lessons and possibly identify any ship-specific issues that need to be evaluated further and recorded;
- Member States encourage companies to ensure that:
  - All participants are fully aware of their duties and responsibilities before participating in a drill or exercise;
  - An oral review and debriefing on the outcome takes place following a drill or exercise. This should include consideration as necessary of changes to procedures in the SSP, identification of gaps in the channels of communication and the need for authorities to intervene.

It is a **good practice** that

- Security drills and exercises are implemented as part of a multiannual training programme that evolves in complexity considering the outcomes of each activity conducted.
- Cybersecurity drills and exercises should be considered as part of the security exercise and training programme.

5.10. Records

Records are essential to provide evidence of compliance with the requirements of the Regulation[36].

It is **important** to recall that:

- The period for which records must be retained on board must be specified by the Administration;
- Records must be kept on board and made available upon request by the port State (PSCOs and/or DAOs)[37];
- Records should be kept in the working language(s) of the ship; if the working language(s) is(are) not English, French or Spanish, a translation into one of these languages shall be included[38];

[36] Reg. 725/2004 Annex II Part A 10
[37] MARSEC Doc. 7510 rev FINAL
[38] MARSEC Doc.2702

- Records of exercises kept on board cover feedback and discussion of exercises in which the ship may not have participated.

It is **recommended** that:

- The period for which records must be retained on board is specified in the SSP;
- Records are kept together for ease of retrieval and referral;
- Records are retained for either three years (the maximum time interval between verifications) or five years (to complete a cycle between renewal verifications);
- As part of the security records, a security logbook is maintained in which all security activities are recorded.

5.11. Verification

Once a SSP has been approved, it is necessary for the Administration to verify that the related security system is being implemented and that the associated security equipment is fully functional[39].

It is **important** to recall that:

- The term “fully complies” in ISPS A/19.1.1.1 and A/19.1.1.2 means that a certificate cannot be issued unless all the requirements of the approved SSP are fully implemented and any associated security equipment and systems are present and in use as required;
- The Administration or a RSO should therefore verify that all security equipment and systems on board are maintained and functioning as intended during any verification. If this is not the case, the deficiencies must be immediately rectified, and this rectification must be sanctioned by the Administration[40];
- If deficiencies are identified during an intermediate or additional verification, the ship must, in the impossibility of immediate rectification, implement equivalent, temporary measures that are at least as effective as those mandated in the SSP and have been agreed by the Administration.

It is **recommended** that:

- Verifications are based on objective evidence obtained through interviews, observation of practices and examination of documents and records (including any internal audit reports) and the functioning of the security equipment, which will enable the Flag State Inspector (FSI) or the RSO security auditor to conclude whether the system complies with requirements of the ISPS Code;
- Intermediate verifications still cover the full scope of the approved SSP and related procedures;

[39] Reg. 725/2004 Annex II Part A 19

[40] Reg. 725/2004 Annex II Part A 19.1.1

- A sample of the reported deficiencies is checked to verify that the Company is investigating, analysing, and resolving those deficiencies efficiently and in a timely manner;
- Particularly for certain ship types – such as Ro-Ro ferry – where some security activities are shared with the port facility, the FSI/RSO checks that:
  - SSOs are fully aware of the extent of the shared responsibilities for controlling access to the ship in conjunction with the port facility; and
  - The SSO has available on board the contact details of the PFSO and has successfully made contact;
- When amendments are made to an approved SSP, their implementation is checked and verified. This verification should cover every amendment to the approved SSP that has been approved by the Administration since the previous verification audit, or since the SSP was originally approved. Additional verifications on the implementation of amendments may be carried out upon the instruction of the Member State;
- The FSI/RSO is in a position to categorise specific findings according to their seriousness;
- Findings are reported in a clear, concise manner and supported by objective evidence;
- Any deficiency is explained to the SSO once the verification has been completed.

It is a **good practice** that ✓

- For officers carrying out verifications to be trained in audit techniques and ISO standards in order to be able to assess effectively the implementation of measures, procedures and duties as indicated in the SSP and the verification of suitable records, considering the need to take into account the differences between a Quality System and the Security System;
- The Administration defines the circumstances when an additional verification is required;
- Procedures are in place to ensure that the certificate is issued with no undue delay.

5.12. Certification

The issuing of an ISSC[41] to a ship follows an onboard verification, during which it is confirmed that a security system and associated security equipment fully comply with the Regulation and the SSP.

It is **important** to recall that:

[41] Reg. 725/2004 Annex II Part A 19.1.1.1 and 19.2.1

- An ISSC cannot be issued based on a verification carried out prior to the approval of the applicable SSP;
- In the case of interim ISSC (IISSC), it shall be verified that the SSP submitted for approval is being implemented on board;
- A RSO cannot use activity carried out on a ship on behalf of a previous flag State for the purpose of certification of the ship under a new flag State;
- An ISSC cannot be issued prior to the related initial or renewal verification;
- An IISSC shall not be issued to a ship from which an ISSC has been withdrawn;
- Issuing consecutive IISSCs is considered an exceptional measure and should not be used to avoid full compliance with the requirements of the Code;
- For the purpose of certification, neither the Regulation nor the Code establish different gradings of failures of security equipment or systems. Therefore, certification cannot be conditional or qualified.

👍 It is **recommended** that:

- Member States ensure that when they issue electronic security certificates, said certificates are supported by an established procedural framework that takes into account IMO FAL.5/Circ. 39 as revised;
- Administrations ensure that officers responsible for the verification/certification process are adequately guided on how to assess and report any failures they identify in such process;
- Member States establish clear conditions under which a ship that has been declared by the Company as out of service or in lay-up, will have its ISSC suspended or withdrawn (MARSEC Doc. 3205 Annex 4 Rev.3).

5.13. Control of ships by the Flag State

Member States have the primary responsibility to put in place an adequate and effective system to exercise control over ships flying their flag and to ensure that these comply with relevant international rules and regulations in respect of, *inter alia*, maritime security[42].

Since there is no standard and common system in place for the control of maritime security activities of own flagged ships, each Member State must develop its own control system to ensure conformity of its ships with maritime security requirements.

It is **important** to recall that:

- Control is carried out by Member State officials and cannot be delegated;
- Verifications carried out for certification purposes constitute an administrative task, and not a control activity. Of course, during an intermediate or an additional verification, an element of control may be included but only if carried out by FSIs;

[42] United Nations Convention on the Law of the Sea (UNCLOS) article 94

- Control can result in the imposition of sanctions. Hence, Member States shall develop a system to ensure that ships flying their flag are subject to control and sanctions in case of non-compliance (infringements).

It is a **good practice** that in relation to national flagged ships, Member States use the following resources for the implementation of control systems ✓

- A system of regular flag State inspections for ships calling at national ports;
- A network of FSIs to be based on selected ports abroad for this purpose;
- A system of global reach for FSI inspections, with FSIs travelling to other countries as results necessary;
- A system of ad hoc FSI travel to inspect ships in cases of serious findings by PSCOs or information from RSO verification reports; and/or
- The organisation of short or longer period inspection campaigns.

5.13.1. Requirements for internal audits

Internal audits are part of the process for the CSO and SSO to monitor the continuing relevance and effectiveness of a ship security plan. A SSP must set out the procedures for auditing the security activities of the ship.

It is the responsibility of the company security officer to arrange for internal audits of security activities, and ensure that deficiencies and non-conformities that have been identified are properly addressed. Records must be kept of internal audits that have taken place.

It is reminded that personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation must be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship[43]. The decision on the extent of impracticability of said provision should be taken by the Administration that has approved the ship security plan[44].

👍 It is **recommended** that:

- Internal audits are carried out at least once a year;
- Internal audits be carried out in case of additional verifications and/or detention on security grounds;

[43] Reg. 725/2004 Annex II Part A 9.4.1 (the Commission and EMSA are aware that this generally only applies to the Company)

[44] MARSEC Doc. 7705

- Criteria should be established by the Administration approving the SSP to determine when it is impracticable for a Company (or a ship), due to its size or nature, to maintain the independence of the internal audit activities.

5.14. Delegation of tasks to RSOs on ship security

RSOs[45] are organisations, with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorised to carry out assessment, verification, approval or certification activity.

When Member States decide to give such authorisations, they select which organisations will be entrusted to act on their behalf for the purposes of maritime security and provide the said organisations with instructions on any flag State specific issues – such as security threats – that must be considered when carrying out SSAs, preparing SSPs and conducting onboard verifications as applicable.

5.14.1. Authorisation of RSOs

RSOs are directly appointed by the Flag Administration.

It is **important** to recall that:

- In terms of criteria for their appointment, RSOs need only to comply with ISPS B/4.5, which is mandatory under the Regulation;
- Directive 2009/15/EC of 23 April 2009[46] on common rules and standards for ship inspection and survey organisations does not apply to ROs when acting as RSOs;
- When changes occur in the framework of RSO delegation, these have to be duly communicated to the European Commission and the IMO.

It is **recommended** that:

- The Member State provides the RSO with full legislation related to the delegated activities and keeps the appointed RSO updated with any changes in such legislation;
- For the Member State to grant authorisation, to the RSO should:
  - confirm that all its security personnel have had appropriate security vetting;
  - make available completed verification and certification files;
  - provide full access to its database;
  - commit to notify changes to procedures and standards directly related to the delegated tasks (Member States should establish whether any such changes should be subject to prior agreement).
- When authorising a RO as a RSO, Member States:
  - establish a clear distinction between the roles of RO and RSO in the “Agreement”;

[45] Reg. 725/2004 Annex I reg 1.16
[46] and Regulation (EC) No 391/2009 of the European Parliament and of the Council of 23 April 2009

  - clearly define the tasks delegated to the organisation as RSO in the Agreement;
  - notify the delegated tasks to the IMO and the Commission.
- When referring in the Agreement to the tasks delegated as RSO, a reference to the Regulation is included;
- Member States issue guidance to RSOs on the conduct of the verification-certification of ships. In this regard it is important to ensure that the procedural requirements adopted by the RSOs are in line with the regulatory requirements of the ISPS Code and the national requirements.

It is a **good practice** that

- Member States agree with RSOs about the failures that should be notified to said Member States when so identified in the course of verifications;
- Member States agree with RSOs which RSO offices will be designated as points of contact for security matters related to the delegated tasks.

5.14.2. Monitoring and controls of RSOs by Member States

It is essential that Member States monitor the RSOs they have appointed to ensure they are carrying out the maritime security tasks delegated to them effectively and in accordance with the regulation.

It is **important** to recall that:

- Monitoring needs to be carried out irrespective of whether the RSO has carried out any delegated tasks or not. In cases of lack of activity, said monitoring should, as a minimum ensure that the RSO continues to meet the criteria for its appointment.

It is **recommended** that:

- Member States develop an oversight regime of regular monitoring of their RSOs which could include:
  - Regular RSO auditing that would not be limited to the RSO’s office(s) in the Member State, but also address other components of the RSO producing activities on behalf of the auditing Member State;
  - Tracing the maritime security activity of the RSOs through their databases;
  - Verification report reviews on a sampling basis;
  - Attendance by FSIs of sample verifications carried out by RSO auditors;
  - Inspections by FSIs of ships recently verified by RSOs on a sampling basis;
  - Following up RSO-related failures identified during RSO verifications or Port State Control or DAO activity.

5.14.3. SSP approval

Where Administrations delegate the task of SSP approval to RSOs,

It is **important** to recall that:

- The RSO that has either prepared the SSA or the SSP of a particular ship cannot approve that SSP or amendments thereto[47].

👍 it is **recommended** that Member States:

- Provide the RSO with clear written instructions on which amendments require prior approval and which do not;
- Randomly review the approval of SSPs carried out by RSOs (for accuracy and consistency (a minimum annual level of inspections could be envisaged).

5.15. Company Security Officer

This section has not been developed at this stage.

5.15.1. Qualifications and training

This section has not been developed at this stage.

5.15.2. Specific duties

This section has not been developed at this stage.

5.15.3. Requirements for internal audits

This section has not been developed at this stage.

[47] Reg. 725/2004 Annex II Part A 9.2.1

6. Control of Ships by the Port State

It is the responsibility of the Member States to ensure that foreign flagged ships calling ports within their territory comply with SOLAS XI-2 and the ISPS Code. The control is twofold:

- Control of ships in port;
- Control of ships intending to enter the port.

In both cases the control is carried out by Duly Authorised Officers (DAOs), legally authorised to exercise control and compliance measures on security grounds.

It is **important** to recall that:

- DAOs have the right to go on board the ship to verify that required certificates are in proper order;
- PSCOs approach to maritime security control on foreign flag ships in port might differ from the DAOs in the initial scope, under the applicable Port State Control MoUs and relevant EU legislation (i.e. Directive 2009/16/EC of the European Parliament and of the Council of 23 April 2009 on Port State Control[48]). Nevertheless, both PSCOs and DAO must check maritime security aspects[49].

The main difference between DAO and PSCO functions is that DAOs have direct legal authorisation to exercise express control and compliance measures according to SOLAS XI-2/9. When, within their PSC functions, PSCOs establish clear grounds for maritime security, they must – unless authorised as DAOs themselves – call the competent authority (DAOs) to take over.

it is **recommended** that:

- In exercising its obligations under SOLAS XI-2/Reg 9, a Member State establishes a control system based on its needs and:
  - Determines scope, structure and composition of the system, defining clear lines of responsibility of all involved;
  - Establishes operating procedures and practices;
  - Records and reports their activity
  - Establishes a minimum annual percentage of ships calling the port that should undergo DAO inspections.

[48] Art. 15, and Annex VI which refer to Instruction 37/2004/10 "Guidelines for Port State Control Officers on Security Aspects" which themselves refer to MSC/Circ. 1111 "Interim Guidance on Control and Compliance Measures to enhance Maritime Security".

[49] MARSEC Doc. 2802

- when DAOs need to check the validity of a ship's certification, the following should be verified:
  - In the ISSC/IISSC certificate itself:
    - The issuing authority;
    - The RSO acting on its behalf (as applicable);
    - The dates on which the verification(s) was carried out;
    - The dates of issue;
    - The expiry date;
    - Its endorsements.
  - If the RSO has issued the ISSC/IISCC certificate, that said RSO is recorded in the IMO GISIS databased as having been authorised by the ship's flag;
  - That an approved SSP is on board;
  - That the date of approval of the SSP is consistent with the ISSC/IISSC certificate;
  - That the data provided in the ISSC/IISSC is consistent with the DOC and SMC;
  - The dates of registration in the flag, the ISM Company, IMO Company number and the Contracting Governments (or RSOs) which issued the certificates, as provided in the CSR.
- When a control activity is conducted, the Master/SSO is provided with a report on the activity carried out[50],
- In the event of imposition of a control measure after clear grounds are established the Master and the Administration concerned are immediately notified.
- In the case of notification under Article 16 of the Regulation 324/2008, a Member State, which is the Port State, should exercise the control and compliance measures in accordance with the Regulation[51]. Article 16 serves as an alert for the concerned Member States who should verify if the security situation on board is satisfactory and, if not, they should act in accordance with the provisions of the Regulation[52].
  -

In light of the above, a notification under Article 16 of the Regulation 324/2008 does not automatically mean that the ship is banned from a port / port facility. Relevant control and compliance measures in accordance with Regulation shall be applied. Denial of entry into port or ship's expulsion from port is dealt with by Annex I 9.3.3 and Article 3.5, indent 11 of the Regulation. Account should be taken of the provisions of paragraphs 4.29 – 4.44 of Annex III. (MARSEC Doc. 2905)

[50] THETIS-EU MARSEC Module may be used.

[51] Reg. 725/2004 Annex I reg 9

[52] Reg. 725/2004 Annex I reg 9.2.5

6.1. Duly Authorised Officers

Duly authorised officer (DAO) means an official of the Contracting Government duly authorised by that Government to carry out control and compliance measures in accordance with the provisions of the Regulation[53].

The security system for controls on ships is based on the activities of DAOs, who must be appointed by Member States to exercise control and compliance measures (MARSEC DOC 5610).

Whilst the professional backgrounds of DAOs may vary, they need to have appropriate knowledge of the provisions of SOLAS XI-2 and of the ISPS Code, of shipboard operations and to be appropriately qualified and trained to the level required by the functions that they are authorised to carry out.

PSCOs may also be DAOs[54], but if this is the case, they should have received additional training and expertise in security matters to become DAOs.

It is **important** to recall that:

- DAOs must be appointed to exercise the control and compliance measures on ships as set out in the Regulation as previously referred, and be issued with identification documents confirming their authority;
- Member States must establish procedures whereby the authenticity of a DAO identification document may be verified[55].

It is **recommended** that:

- Member States take into account the recommendations set out in MSC.1/Circ. 1111, Annex 2, Chapter 2 with regards to qualifications and training of DAOs. Principally, DAOs should:
  - Be knowledgeable with shipboard operations;
  - Receive appropriate training for the functions that they are authorized to carry out;
  - Be able to communicate in English with the Master, the SSO and the officers of the ship;
  - Receive appropriate training to ensure proficiency in safety procedures when boarding ships or on board the ship;
  - Periodically undergo training in order to update their knowledge.
- The identity cards issued to DAOs include tamper-proof features such as holograms, and contact details of the issuing authority;

[53] Reg. 725/2004 Annex I reg 9
[54] Directive 2009/16/EC Annex V B.2
[55] Regulation 725/2004, Art. 3.5 and Annex III, Part B section 4.18

- When DAOs are determining their own control activity, the data in the THETIS-EU MARSEC Module be consulted for information about previous control activities (MARSEC Doc. 7110);
- Clear instructions are provided to the DAOs on how to proceed in relation to the notification to the Administration and the RSO in case of the imposition of a control measure;
- The Member State monitors the activity of its DAOs as way of ensuring consistency in the approach and the quality of their activity;
- As a way of exercising DAO activity Member States may - apart from the conduct of inspection activity triggered by the establishment of clear grounds - consider the establishment of a more structured inspection activity based on a risk-based approach.

It is a **good practice** that ✓

- DAOs participate in specific training activities organised by EMSA.
- DAOs record security inspection reports in THETIS-EU MARSEC Module.

6.2. Pre-arrival information

Member States must require ships intending to enter their ports to provide pre-arrival security information[56]. The competent authority for maritime security makes the choice of how and by whom this information will be processed in first place. Member States shall ensure that the information is made available to their DAOs for them to decide whether a ship should be subject to control.

It is **important** to recall that:

- Member States should check that the pre-arrival information is complete and is analysed before the ship enters port[57].

It is **recommended** that:

- The analysis of pre-arrival information includes:
  - Checking that the list of the last 10 calls at port facilities includes respective LOCODES and port facility IDs;
  - The identification of any port facility called at by the ship, that was at a security level higher than 1;
  - Whether there are any links between the security level of the port facility reported and information related to the security level of the country of that port facility;

[56] Reg. 725/2004 Art. 6.1
[57] Directive 2010/65 Annex A.5

  - Examination of any additional information related to security incidents reported by the ship;
  - Confirmation that appropriate ship security procedures were maintained during any ship-to-ship activity in the period covered by its previous ten calls at port facilities.
- If the review of pre-arrival information raises concerns, the DAO takes into consideration the list of clear grounds in ISPS B/4.33 when deciding to exercise control;
- Member States should not exclusively rely on automated systems to evaluate pre-arrival information other than to confirm that all the information requested has been provided.

6.2.1. Exemption from the provision of pre-arrival information

It is **important** to recall that[58]:

- When a ship is exempted from providing pre-arrival information for a certain scheduled service or route, this does not mean that this ship is exempted for other scheduled services or routes[59];
- The exemptions need to be checked on a regular basis

6.3. Security Inspections

Where clear grounds are identified, the DAO may decide to conduct an inspection as a control measure[60]. This process entails the conduct of the actual inspection work and the related reporting thereon.

6.3.1. Carrying out an inspection

It is **important** to:

- Ascertain the validity of the ISSC/IISSC certificate as indicated above (Section 6 “recommendations”) when clear grounds were established prior to boarding the ship;
- Note that if a ship is not flying the flag of an EU Member State it might not need to comply with the mandatory requirements of Part B of the Code made mandatory by the Regulation.

It is **recommended** that

- After confirming the existence of a valid certificate on board, the DAO takes into account the following:
  - The crew list, to be able to identify personnel certified in accordance with the STCW Convention and Code (STCW VI/5 and VI/6);

[58] Reg. 725/2004 Art. 7

[59] MARSEC 4107-Rev

[60] Reg. 725/2004 Annex I reg 9.1.

  - Records of:
    - The last ten calls at port facilities, including any ship-to-ship activity;
    - Access to the ship;
    - Any DoS;
    - Any changes in security level;
    - Drills and exercises carried out;
    - Records of security incidents (including cybersecurity ones);
    - Maintenance of security equipment (SSAS, cameras, detectors, etc);
    - Crew familiarisation with security duties.
- If the only means to clarify the clear ground(s) is through the content of the SSP and this access is refused by the Master, the DAO should use all means to liaise with the Administration to get the access to the SSP or the attendance on board by the RSO as appropriate.

It is a **good practice** that ✓

- Check that the security level at which the ship is operating is at least that set by the Contracting Government for the port facility as required by SOLAS XI-2/4.3;
- Confirm and cross check, when needed, whether the ship has taken additional measures both in the current and last ports of call;
- Make an initial assessment of the security measures being taken by the ship upon boarding;
- Examine specific security aspects when boarding the ship and moving around:
  - Access to the ship;
  - Access to restricted areas, keeping in mind that the management of restricted areas is confidential and, as long as there are comprehensible reasons, it cannot automatically be assumed that they have to be locked at all times;
  - Monitoring of the security of the ship;
  - Delivery of ship stores;
  - Handling of cargo and/or unaccompanied baggage, if applicable.
- In case the Administration is not reachable after clear grounds are established and these were not clarified, rectified or otherwise addressed to satisfaction, the DAOs should suspend the inspection and use their judgement as to the need or otherwise to impose further control measures.
- Confidentiality issues should be considered related to the inclusion of the cyber risk management in the ISM (IMO resolution MSC.428(98)).
- Member States establish a procedure to record DAOs' security inspections activities in THETIS-EU MARSEC Module.

6.3.2. Control and compliance measures

This section has not been developed at this stage.

6.3.3. Reporting and recording

It is **important** to recall that:

- DAOs are obliged, in the event of a control measure other than a lesser administrative or corrective measure is imposed, to notify:
  - The Administration;
  - The RSO which has issued the certificate of the ship, if applicable;
  - The IMO.

It is **recommended** that:

- Upon completion of an inspection of a ship, the Master is given a report on the results of the inspection, details of any action taken by the DAO, and a list of any non-compliances to be rectified;
- Member States use the form attached in MSC/Circ.1111, for an inspection on clear grounds;
- The results of the inspection be recorded in the THETIS-EU MARSEC Module;
- In case of delay to the ship, restriction of operations or detention to the ship or expulsion, the report is send by the most expeditious means possible.

7. Port Facility Security

Note: port security under Directive 2005/65/EC is covered under points 8 to 11 below.

Regulation 725/2004 and its annexes (SOLAS Chapter XI-2 and the ISPS Code) are the legal instruments regulating maritime security requirements for port facilities (SOLAS XI-2/10) in the EU due to the interface with ships during port / ship operations. In the field of port security, it is important to note that SOLAS refers only to port facilities as distinct from ports in general.

The regulatory approach to port facility security is similar to that applied to ships, dealing with risk assessment in the Port Facility Security Assessment (PFSA) and prescriptive requirements such as a Port Facility Security Plan (PFSP) with its implementation and with designated persons such as the PFSO. A description of the process, the parties involved, and their responsibilities might be found in the figure.

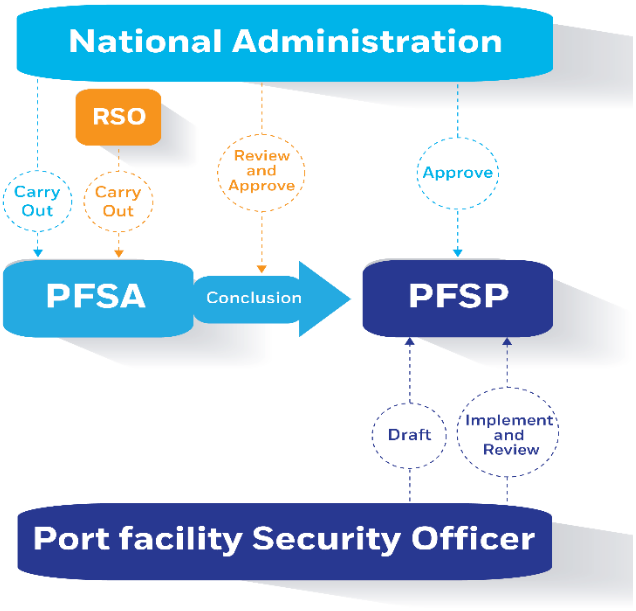

Figure 1. Description of the PFSA/PFSP 5-year cycle

7.1. Port Facility Security Assessment

The base document to set the framework in Port Facility Security is the PFSA which needs to cover all the relevant elements indicated in the Code, namely the identification of assets, threats, likelihoods, countermeasures and weaknesses. This assessment is reflected in a concluding report.

7.1.1. Content and approval

The process starts with the identification and evaluation of assets to protect, including the geographical definition of the scope of the assessment. Threat scenarios would be security incidents that need to be thoroughly studied and charted with regards to their likelihood to happen and subsequent consequences if they occur. The resultant security risk chart for each of the incidents indicates that they are of such gravity as to need effective countermeasures either human or physical.

It is **important** to recall that:

- PFSAs, after considering all applicable threats and identifying all applicable countermeasures, still need to identify any residual weaknesses which must feature in the plan;
- PFSAs are to include within their scope radio and telecommunication systems, including computer systems and networks;
- PFSAs need to be reviewed at least every 5 years and whenever there are changes in the port facility;
- Member State Designated Authorities can delegate the development of PFSAs. However, the approval cannot be delegated;
- The PFSO should not be involved in the administrative steps required for the approval or review of PFSAs, and should only be involved in the development of the PFSA to provide information where required;
- A PFSA must set out conclusions. These should be communicated to the PFSO, and RSO where applicable, to help prepare any required modifications of the PFSP;
- It is to be ensured that both countermeasures and any actions intended to mitigate vulnerabilities identified in the PFSA report are addressed in the related PFSP.

👍It is **recommended** that:

- The PFSA includes a precise map providing a graphic description of the geographical scope of the assessment.
- The PFSA is kept as simple and clear as possible, in order to minimise the administrative burden associated to its conduction and approval;
- The PFSA is conducted taking into account input from the Administration and relevant stakeholders involved;
- The PFSA includes an on-site visit;
- PFSAs take into consideration the cybersecurity dimension, taking into account the reliance on technology of interfaces between port facility and outside networks and between port and ship;
- Authorities commit to issuing PFSA approvals within a reasonable timeframe. A time frame of not more than 3 months for the authorities to answer a request for approval of a PFSA (whatever the answer) shall be considered as reasonable.

It is a **good practice** that ✓

- Conducting a specific cybersecurity vulnerability assessment as an enhancement to the generic PFSA;
- Introducing cyber resilience architecture in the design of new networks for PFs;
- Using a geographic information system (e.g. Google maps, OpenStreetMap) to provide a graphic description of the geographical scope of the assessment and the location of the different assets.

7.1.2. Reviews and amendments to a PFSA

If business activities change or if there are some changes in the port facility infrastructure, the PFSA may need to be revised. Changes which require a revision can include modifications of the perimeter of the port facility, modification of the type of operation and/or operator, modification of the restricted areas, etc. Furthermore, PFSAs need to increasingly take into consideration the cybersecurity dimension, considering the reliance on technology of interfaces between port facility and outside networks and between port and ship.

7.2. Port Facility Security Plan

Port Facilities under the scope of the Regulation need to have an approved PFSP based on the results of the PFSA.

It is **important** to recall that:

- A PFSP should be developed and maintained on the basis of a PFSA. If the review of the PFSA impacts on the provisions of the PFSP there must be a subsequent review of the plan;
- A PFSP should include measures intended to address the interface between the port facility and ships allowed to call at it and that are out of the scope of the Regulation;
- The coverage of monitoring of waterside areas, Single Point Moorings (SPMs), and berthing areas is mandatory;
- Security services subcontracted to or provided by third parties must be under the control of the PFSO according to the provisions of the PFSP. If direct control is not possible, a written agreement considering the different aspects of the relation with the service provider should give the PFSO the adequate level of control;
- If some requirements of the PFSP are addressed with external documents (in particular standing operating procedures of a security provider for their employees serving at the port facility) there must be a clear reference to these documents in the plan and these external documents considered part of the plan.

👍 It is **recommended** that:

- If a private company is assigned to perform specific security duties in the port facility, the related agreement for services details the procedures to be performed in such a way as to ensure clarity between such procedures and the parts of the PFSP they are intended to fulfil.
- The PFSA provides a static picture of the security of the port facility at a given time. The PFSP must be based on the PFSA in such a way that the measures determined in the PFSP address the issues found in that picture. Considering this, there should be a timely link between the PFSA and the subsequent PFSP. Consequently, it is recommended that the National Administration establishes a maximum time span for the validity of the PFSA. It would be advisable that the time span between the adoption of a PFSA and the drafting or revision of the PFSP does not exceed 4 months.

7.2.1. Content and approval

It is **important**:

- To verify that the PFSP addresses all the mandatory requirements, including those made mandatory by the Art. 3.5 of the Regulation[61];
- To verify that the PFSP is consistent with the PFSA, ensuring that all the issues identified by the PFSA are addressed through specific security measures in the PFSP;
- That Member States determine which changes in an approved PFSP shall not be implemented unless the relevant changes are approved by the Authorities. In this regard, the PFSO can implement all necessary changes and updates to the PFSP. The competent authority at their periodical review of the PFSP will review the updating and changes. Minor changes to the PFSP shall be reviewed and included at annual updating of the plan. It should not be required to reissue the PFSP for approval when minor changes are implemented. Upon major changes (e.g. modifications of the perimeters of the PF, changes in the access control and relevant countermeasures/gates layout, modification of the restricted areas, inclusion of an area dedicated to the storage of dangerous goods, etc.) the PFSP shall immediately be sent in for new approval by the competent authority[62].
- For the services of a Member State to have the necessary expertise to approve a PFSP;
- That the PFSP contains appropriate provisions to ensure that security is not compromised by activity with any ships that are not subject to the ISPS Code[63] , in particular inland waterway vessels (i.e. barges)[64].

[61] Reg. 725/2004 Annex III Part B sections 16.3 and 16.8
[62] MARSEC Doc.7408 Final and Regulation 725/2004 Annex II Part A 16.6
[63] Reg. 725/2004 Article 3.8
[64] See MARSEC Doc. 8709 for examples of practices relating to non-ISPS ships in ISPS port facilities

It is **recommended** that:

- Authorities commit to issuing PFSP approvals within a reasonable timeframe. A time frame of not more than 3 months for the authorities to answer a request for approval of a PFSP (whatever the answer) shall be considered as reasonable;
- All security measures applied at the port facility are recorded in the PFSP (including specific instructions, if any, from the external security provider to their employees;
- The PFSP includes an index of contents;
- Measures are taken to guarantee at all times the authenticity and integrity of the PFSP.

It is a **good practice** that ✓

- Using a geographic information system (e.g. Google maps, OpenStreetMap) to provide a graphic description of the geographical scope of the plan and the location of the different assets.
- Within the procedures for reporting security incidents that must be included in the PFSP especial mention is made to the reporting of cybersecurity incidents.

7.2.2. Reviews and amendments to a PFSP

It is **important**:

- That Member States determine which changes in an approved PFSP shall not be implemented unless the relevant changes are approved by the Administration;

It is **recommended** that:

- The plan allows proper traceability of amendments. If amendments have been made to the PFSP, a record of changes should identify these amendments, so that, at any point in time, the PFSO can be in a position to know what is new and the history of the plan is traceable;

7.3. Port Facility Security Officer

It is **important** to recall:

- Port Facility Security Officers (PFSO) obligation to report and to maintain records of occurrences which threaten the security of the port facility including cybersecurity incidents[65].

[65] Reg. 725/2004 Annex II Part A 17.8

7.4. Restricted Areas

This section has not been developed at this stage.

7.5. Security equipment

This section has not been developed at this stage.

7.6. Qualifications and trainings

The port facility personnel without and with designated security duties should, before being assigned such duties, receive familiarization training in their assigned duties and responsibilities taking into account the relevant provisions of the port facility security plan. Apart from the participation to the quarterly Drills and annual Exercises, it is considered a good practice to organise periodical trainings and familiarization through conferences on security topics and/or arranging ad-hoc computer based learning programs, tailored for the specific port facility, duly created to be carried out online through a PC platform, taking into account MSC.1/Circ.1341 on 27 May 2010, "GUIDELINES ON SECURITY-RELATED TRAINING AND FAMILIARIZATION FOR PORT FACILITY PERSONNEL and their annexed Table1 and Table 2 "Knowledge, Understanding and proficiencies (KUPs)".

It is a **good practice** that ✓

- Cybersecurity training at different levels is considered as part of the security training programme in order to create a cybersecurity culture across the organisation.
- Introducing the figure of the Chief Information Security Officer (CISO) in the organisation to ensure that cybersecurity threats are considered, adequate preparedness measures are taken, and suitable response and recovery procedures can be implemented if necessary.

7.7. Drills and exercises

Security drills are intended to be held periodically to test individual elements of a PFSP and should establish that port facility personnel are alert and proficient and that the PFSP is being implemented properly. Further information on this topic might be found in the Exercitium[66].

Drills are usually small, operational practices designed to test a specific part of the security plan. Drills allow crew or staff to introduce, test or practice a procedure, task or routine related to their security role (e.g., baggage search, use of security equipment, implementing a particular measure at a higher security level). *To ensure the effective implementation of the provisions of the security plan, drills should be conducted at least every three months […]*[67].

Exercises are organised on a larger scaleand are intended to test the wider context of a security system described in the plan, including communication, coordination, availability, resources, and reactions. *Various types of exercises, […], should be carried out at least once each calendar year with no more than 18 months between the exercises*[68].

Exercises are usually not limited to the port facility but include the participation of other stakeholders such as relevant authorities within the Administration responsible for maritime security, ships and management companies, other port facilities and port authorities.Exercises do not always need to be operational. Equally successful can be a “table-top exercise” where the main security issues of cooperation are reviewed and updated. There should be a balance between the different types of exercises.

Workshops and seminars differ conceptually from drills and exercises. **Workshops** gather stakeholders to develop security plans and procedures through consensus[69]. **Seminars** gather participants to inform about existing procedures.

Nevertheless, even if seminars and workshops are not intended to test the plan as drills and exercises do, with the adequate content they might count as a type of annual exercise in the context of the Regulation[70] (ref Annex III Part B 13.7.2). It should always be taken in consideration that the multiannual plan maintains an adequate balance between the different types of exercise.

It is **important** to note that[71]:

- The goal of the exercises is to test communication and coordination among stakeholders;
- The minimum frequency for drills is three months while that for exercises is every calendar year, not exceeding eighteen months between them;

[66] Exercitium. European Handbook of Maritime Security Exercises and Drills.
[67] Regulation 725/2004 Annex III Part B 13.6 for Ships and 18.5 for Port Facilities (mandatory as per art. 4.5)
[68] Regulation 725/2004 Annex III Part B 13.7 for Ships and 18.6 for Port Facilities (mandatory as per art. 4.5)
[69] In addition, “workshop” is not a term used or recognised in Regulation 725/2004
[70] Regulation 725/2004 Annex III Part B 13.7.2 for Ships and 18.6 for Port Facilities (mandatory as per art. 4.5)
[71] Regulation 725/2004 Annex III Part B 18.5 and 18.6

- Drills can be computer-based as long as the threat scenarios which are presented are related and specific to the PFSP, in order to test individual elements of the plan. However, not all threat scenarios can be computer-simulated, and a balance needs to be found with live, operational drills, in order to verify the readiness and reactivity of security personnel.

👍 It is **recommended** that:

- Drills and exercises keep in focus the threats identified in the PFSA and for which measures approved by the Administration are described.
- Drills and exercises are included in a multiannual plan with the right balance of table-top and operational events. This multiannual plan should be regularly reviewed to accommodate lessons learned and training needs identified.
- Long-term planning is necessary to integrate exercises within other security preparedness activities creating a multiannual schedule and improving cycle as shown in the figure. In addition, local exercise planning could be incorporated into national and international preparedness activities. Security exercises may be integrated within major exercises containing other elements such as safety or antipollution elements. Indeed, complex incident scenarios (e.g., a bomb on board a ship berthed at a port facility explodes, causing a fire, casualties, and bunker pollution) are realistic and provide the opportunity to test not only security plans but also the interaction with other plans and response structures. In this context, it might also occur that one or several drills for specific participants are conducted within the context of a major exercise (e.g., crew on board conducts a bomb search drill within an exercise scenario of a terrorist attack in a port). In these cases, it is important that each event is evaluated and reported adequately.

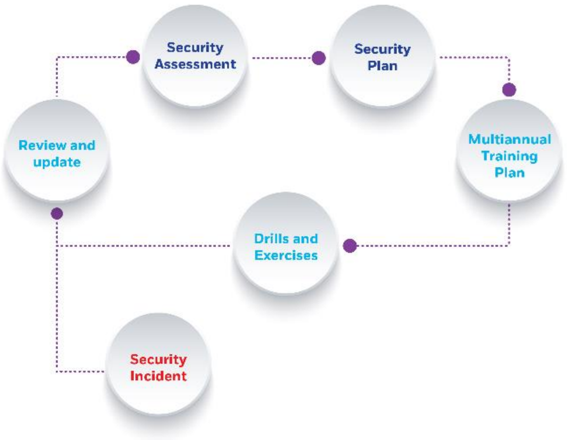

Figure 2. Multianual security improving cycle

- Exercise documentation at least indicates the time of the exercise, the subject of the exercise, the participants or target group and the main findings and conclusions.

It is a **good practice** that ✓

- Security drills and exercises are implemented as part of a multiannual training programme that evolves in complexity considering the outcomes of each activity conducted.
- Cybersecurity drills and exercises are considered as part of the security exercise and training programme.

7.8. Records

Records are essential to provide evidence of port facility compliance with the requirements of the Regulation.

👍 It is **recommended** that:

- Port facilities ensure that their plans include provisions for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements;
- Although it is not mandatory for PFSPs to include minimum time for which security records have to be retained at the port facility, Administrations do establish such minima and give clear instructions to this effect to personnel with responsibilities for record keeping (i.e. PFSO).

7.9. Port facilities occasionally serving ships engaged on international voyages

Not all port facilities are intended to serve ships engaged in international voyages. However, there could be instances where port facilities not intended to serve SOLAS ships may still be used by such ships occasionally. Nevertheless, said port facilities, not subject to have a PFSP, must ensure an adequate level of protection in accordance with the Regulation[72].

It is **important** to recall that:

- It is for a Member State to decide the extent of application of the Regulation to those port facilities within its territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage;
- When it is decided that a port facility occasionally serves ships engaged on international voyages clear rules are established in writing by the authorities at the appropriate level of decision.

[72] Reg. 725/2004 Annex I Reg.10.3

- It is required that a responsible person ashore is appointed to make arrangements with the ship on the security measures to be implemented. This person will be responsible for shore-side security (in lieu of the PFSO) and needs to have a clear authority to agree a DoS with a SOLAS ship intending to engage in a ship/port interface.

👍It is **recommended** that the Member State establishes:

- In carrying out the PFSAs of the port facilities located in their territory, in order to determine which PFs are to be included in the aforementioned case, the following criteria must be taken into consideration by the competent authorities of the Member States:
  - Frequency of the international traffic: a maximum number of ship's calls per year should be determined to berth and undertake commercial operations at the "occasional" port facility;
  - Ship's type: the competent authority might decide to authorize a limited type of vessels, due to the absence of permanent infrastructures (passenger ships, high speed crafts, oil and chemical tankers, gas carriers, MODU, etc.)
- The minimum requirements for a person ashore to be appointed with security responsibilities, including qualifications and experience required for the exercise of related duties, such as:
  - Comprehensive knowledge about ship-port operations;
  - Knowledge of maritime security terms and definitions including comprehensive knowledge of the EU and the IMO regulation(s);
  - Knowledge of the maritime security levels and the consequential security measures and procedures aboard ship and in the port facility environment;
  - Knowledge of the requirements and procedures for reporting deficiencies, and the requirements and procedures for security-related contingency plans;
  - Knowledge of the Declaration of Security (DoS);
  - Language skills particularly in English;
- 24-Hr contact details of the person responsible to report any security-related incident and to assist the ships in case of need.

7.10. Inspections and controls of Port Facilities

Within the current Maritime Security regulatory regime, there is no standard or common control system in place for maritime security activities for port facilities. In order to assist the competent authorities in the Member States however, the Commission services have developed a checklist to facilitate verifications of port facilities[73].

[73] MARSEC Doc. 7908, Annex II (MARSEC Doc. 7910)

It is **important** to recall that:

- Member States should develop a system for controlling the maritime security activities in its port facilities[74]. The national system developed must be adequately implemented;
- Control can result in the imposition of sanctions. Hence Member States should develop a system to ensure that port facilities are subject to control and sanctions in case of non-compliance.
- This means that Member States are responsible and accountable at all time towards the EU, and as a consequence to the Commission, of a thorough enforcement of maritime security measures by port facilities situated within their territories.

It is **recommended** that:

- A port facility inspection programme is developed to verify the implementation and test the effectiveness of the port facility security plan considering the specific monitoring needs for each port facility. Such programme could include regular and ad hoc supervision, and consider other control activities (e.g., on-site visit, participation in exercises).
- Monitoring activities to be recorded so evidence can be presented during inspections.

It is a **good practice** that ✓

- Each port facility is inspected once every year to verify the implementation and test the effectiveness of the port facility security plan.
- Alternatively, the system for controlling the maritime security activities in port facilities includes a need-based inspection programme developed to ensure that the port facilities supporting greater risk are inspected more often. The programme could establish the frequency of inspections in each port facility based on different criteria:
    - Specific characteristics (e.g, size and complexity, number of passengers, type of goods, symbolic value, location).
    - Performance criteria including adequacy of the PFSP and results of previous inspections (e.g., compliance with the regulation, correction of deviations, security awareness of the staff).
    - Five year live-cycle of the PFSA and PFSP (e.g., include an initial inspection following the approval of a new PFSP).

[74] Reg. 725/2004 article 9.1.

7.10.1. Requirements for internal audits

This section has not been developed at this stage.

7.11. Delegation of tasks to RSOs on ort facilities security

This section has not been developed at this stage.

7.11.1. Authorisation of RSOs

This section has not been developed at this stage.

7.11.2. Monitoring and controls of RSOs by Member States

This section has not been developed at this stage.

8. Port Security

Directive 2005/65/EC of 26 October 2005 on enhancing port security extends security to ports as a whole, requiring additional administrative tasks to cover any ‘Port’ in the meaning of any specified area of land and water, with boundaries defined by the Member State, in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations[75].

The objective of the Directive is to improve security coordination in areas of ports which are not covered by the Regulation (EC) 725/2004 and also to ensure that the enhancement of port security can support the security measures taken under the Regulation. Whilst the responsibility for the implementation of security measures at port facility level essentially falls to the port facility operator (in general a private entity), the appropriate security measures at port level are the responsibility of the port authority and of those authorities which are responsible for keeping public order, safety and security measures within the port area (in both, public and operational areas).

The Directive shall apply to every port located in the territory of a Member State in which one or more port facilities covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 is or are located.

A systemic approach should be applied since the port is considered as one complex entity whose security or vulnerability depends on all its components. The study on the Technical Aspects of Port Area Security (TAPS II)[76] could be a useful instrument, in order to redefine the port boundaries in terms of security, including the necessity to take due account of their water side, sea approaches and/or anchorages when required. Moreover, this study focuses on recommendations and methodologies for the efficient application of the Directive and the technical means for its implementation.

Member States shall communicate to the Commission the text of national law that they adopt to transpose the Directive.

It is **important** to recall that:

- Member States shall designate a port security authority for each port covered by the Directive;
- The terms "ports" and "port facilities" shall be treated as **not interchangeable**, in order to avoid confusion as regards the respective requirements of Regulation (EC) No 725/2004 and of Directive 2005/65/EC.

[75] Article 3.1, Dir.2005/65/EC)

[76] Study based on the work undertaken by the Joint Research Centre (JRC) in direct support of the European Commission services

- A Port Security Authority may be designated to cover more than one port. However, this should be clearly mentioned in the PSA and PSP, and this information should be provided with all details.

It is a **good practice** that ✓

- That Member State establishes a **Port Security Advisory Committee**, whose members are representatives of all authorities having a role to play in terms of security and/or in crisis management (i.e. Port Security Authority/Port Security Officer, Coast Guard, Harbour Master office, Police, Border Guard, Customs and other relevant parties as deemed necessary) to act as a security consultative body involved in the continuous development and implementation of the port security plan, in order to ensure better coordination and continuous improvement.

  The purpose of the Port Security Advisory Committee is to provide a framework to communicate, to identify risks and to coordinate resources to mitigate threats and consequences, improve security measures, to make recommendations by identifying the unique characteristics of each port and to help coordinating a rapid response to changes in threats.

  Periodical meetings should be organised by the Port Security Authority – as defined by Art.5 - particularly the occasion of developing and reviewing the Port security Assessments and Plans. The minutes of such meetings should be drafted and retained for an agreed period of time.

- In order to facilitate the Port Security Authority –who might also be the "competent authority for maritime security" provided for under Regulation (EC) No 725/2004 as designated by the Member State - or RSOs in drafting the PSAs and PSPs, Member States should develop specific templates, as well as clear procedures and arrangements necessary for the completion and review of such documents. Properly structured templates should also facilitate the approval process.

8.1. Port Security Assessment (PSA)

The Port Security Assessment is the key first step in the implementation process and should consider the port and its environs - not just those areas within the physical or administrative boundaries - the specificities of different sections of a port and, where deemed applicable by the relevant authorities of the Member State, of its adjacent areas if these have an impact on the security in the port and it should take into account the common essential port elements known as *cohesion elements*[77].

[77] MARSEC 5110-Rev1-Annex "Guidelines for the definition of port boundaries under Directive 2005/65/EC on enhancing port security"

8.1.1. Content and Approval

The Port Security Assessment shall include both a landside and waterside assessment of the port and will comprise a risk assessment of all areas to establish potential threats to the port.

According to the specific circumstances, some ports (i.e. small ports or with a very restricted water access) could have just one water zone but this should be the result of an assessment and should be adequately documented. Busiest and bigger ports are generally provided with a regulated water area (i.e. anchorages, river, canals, traffic separation scheme and other sea areas allocated for lightening and ship-to-ship operations).

The base document to set the framework in Port Security needs to cover, as a minimum, the detailed requirements laid down in Annex I of the Directive, in particular the identification of important assets and infrastructures, possible threats - which may include all different types of security incidents - likelihoods of their occurrences, countermeasures and weaknesses.

Not every shipyard[78] – in particular those exclusively dedicated to new constructions - have to comply with the provisions of Regulation (EC) 725/2004, but may be located adjacent to port facilities and its activities may have an impact on the security of ships using such port and port facilities and more globally on port security. Therefore, the port security assessment shall consider such situation and, as a consequence, specific measures and procedures for the shipyard facility area should be included in the PSP, as appropriate.

It is **important** to recall that:

- PSAs, after considering all applicable threats and identifying all applicable countermeasures, might still need to identify any residual weaknesses which must feature later on in the plan;
- Both countermeasures and any actions intended to mitigate vulnerabilities identified in the PSA are instrumental for the preparation of the related Port Security Plan.
- PSAs shall include the organisational aspects relevant to overall port security, including the division of tasks between all the authorities and forces involved in the port security, and also the existing rules and procedures
- Attention shall be paid to the relationship with other response/contingency plans, even if not prepared or adopted by the competent or designated authorities for maritime security;
- Assets and infrastructures located outside port facilities, but presenting an interest in terms of port security, shall be properly assessed;
- PSAs shall take into account the assessments for port facilities within their boundaries as carried out pursuant to Regulation (EC) No 725/2004[79].

[78] See MARSEC 6609 for further details in different uses of the shipyards and the implications in their compliance with the provisions of the Regulation.
[79] Directive 2005/65/EC Article 6.1 and Annex I

- The approvals of the PSAs are properly documented (letter of approval or a signed copy of the Port Security Assessment)

👍 It is **recommended** that:

- PSAs are conducted taking into account inputs from the Maritime Administration and relevant public and private stakeholders involved in the port operations and security-related activities;
- For the identification of the port personnel subject to background checks, the national legislation of the Member State should be made suitable to allow such checks to take place;
- PSAs increasingly consider the cybersecurity dimension, taking into account the reliance on technology of interfaces between the port and port facilities and external networks (i.e. logistics, intermodal services and systems, etc.);
- PSAs should take into account the PFSAs for the port facilities within the boundaries of the port. There should be particular attention to how the vulnerabilities of individual port facilities can affect the vulnerability of the whole port. For example, the presence of dangerous goods has to be carefully considered throughout the port and not only in individual PFSAs[80].

8.1.2. Defining port boundaries

Member States shall define for each port the boundaries of the port for the purposes of the Directive, with the aim of enhancing port security, appropriately taking into account the information resulting from the port security assessment, including the operational areas, non-operational areas, port infrastructures, waterside and adjacent areas.

The definition of the port boundaries depends on the typology of the port as well as on the type of the terminals, infrastructure, installations, marinas, etc. Member States should take into account the TAPS II Study and the MARSEC Document 5110-Rev1-Annex "Guidelines for the definition of port boundaries".

A good approach for the proper drafting of the port security assessment, including the definition and final delineation of the port security boundaries, should be to start listing and filling data in the 3 different categories of port areas that usually, but not necessarily, are within the administrative port limits (as listed below) and are also mentioned in the conclusions of the "Taps II study", as follows:

- **All port "operational areas"** that basically are all port facilities within the port.
- **All port "non-operational areas"** that are basically zones/areas that are placed outside the port facilities but have some operational access restriction (i.e.; essential port services as water and electrical station supplies, emergency services, port enforcement authorities buildings, VTS towers, pilots station, fishing docks areas, etc. In addition,

[80] See the Study on the Technical Aspects of Port Area Security (TAPS II)

open areas such as i.e. urban areas inside or in the close vicinity of the port such as port shops or malls and marine related business, including yacht marinas and yacht clubs if any should be included in this category

- **Port infrastructures – Waterside approaches – Adjacent port areas are:**
  - **Port Infrastructure** as breakwaters, access channels and locks, port public infrastructure as railways and roads, bridges, tunnels inside or in the close vicinity of the port.
  - **From the waterside,** defined anchorages, maritime lights and beacons, approaches and waterways from seaward.
  - **Finally, the port adjacent areas** that might have an impact on the port operations activities. (i.e. shipyards, oil & gas terminals, factories or industrial installations/warehouses located next to the seashore and in the vicinity of a port, that due to their specific activities and locations might have an impact on the security of that port.

In line with the requirements of Article 2.3 of Directive 2005/65/EC and in order to make an educated decision on the definition and delineation of the port security boundaries of a port for the purpose of this Directive, the competent national authorities in close cooperation with the port security authority are required to properly assess and take due account at least of the following key port security assessment elements and information:

- The list of important port assets and port infrastructures to protect.
- The list of possible threats to the port assets and infrastructures.
- The list of available and future required counter-measures in the port.
- The list of the port weaknesses points, including human factors in the port infrastructure, port and port facilities operating policies and procedures.

It is **important** to recall that:

- The inclusion of certain areas within the port security boundaries does not imply in a systematic manner their protection or the application of access restrictions.
- The assessment shall take into account the variety of situations depending on the implementation of each of the 3 security levels.
- *Non-operational areas* of the port, that basically have some access restrictions should be included within the port boundaries (i.e. essential port services as water and electrical station supplies, emergency services, VTS towers, pilot stations, fishing docks, etc., as well open areas such as urban areas that are located inside or in the close vicinity of the port).

It is **recommended** that:

- The identification of the port boundaries include a visualisation of the areas relevant to port security categorised by port facilities covered by a PFSP and clustered objects, thus allowing also a view to the security competences of the different authorities (Police, Border Guard, Customs, etc.) in those areas that are outside the administrative port boundaries but within the port boundaries in terms of security.

- A written account should be drafted detailing how the port boundary has been established, as well as maps, plans, nautical charts, drawings outlining the port boundaries, including those of the port facilities within the port, that are integral part of the Port security Assessment . The adjacent water approaches to the port must be considered as well as the anchorages areas if already defined.
- Artificial separations between port security boundaries on the basis of economic interests are not acceptable.

It is a **good practice** that ✓

- Using a geographic information system (e.g. Google maps, OpenStreetMap) to provide a graphic description of the geographical scope of the assessment and the location of the different assets.

8.1.3. Conditions for a potential application of the provisions of Article 2.4 of the Directive and consequences thereof.

According to article 2.2 of Directive 2005/65/EC, "*the measures laid down in this Directive shall apply to every port located in the territory of a Member State in which one or more port facilities covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 is or are situated*."

Article 2.4 of this Directive clearly states that " *Where the boundaries of a port facility within the meaning of Regulation (EC) No 725/2004 have been defined by a Member State as effectively covering the port, the relevant provisions of Regulation (EC) No 725/2004 shall take precedence over those of this Directive* ".

We are considering here the case where the port consists of **<u>ONLY</u>** one port facility serving commercial maritime traffic, and this port facility is covered by a PFSP by virtue of Regulation (EC) 725/2004.

In such case the port boundaries have been established as coinciding with the limits of this single port facility as a conclusion of the Port Security Assessment carried out in accordance with its Article 6 and Annex I of Directive 2005/65/EC. The reasoning for any such decision must be clearly demonstrated and documented, on a case by case basis.

Should the port include other elements than a single port facility engaged in commercial traffic and therefore covered by an approved port facility security plan , like facility/ies- moorages-zones of anchorages for fishing or merchant vessels, for recreational boats like a marina, for public services (pilotage, firefighting, Customs, and other law enforcement vessels) etc.., then the provisions of article 2.4 of Directive 2005/65/EC can no more apply.

As a result of such a definition of port boundaries in terms of security, the already existing and approved PFSP effectively covers also the port: a separate PSP would not provide any additional element of protection with regard to the port and the relevant provisions of the Regulation with regard to the PFSP indeed takes precedence over the corresponding provisions of the Directive concerning the PSP.

It is **important** to recall that:

- A PSA shall be outlined in cases where the provisions of Article 2.4 are met, the PSA shall clearly conclude that the boundaries of the port facility effectively cover the port and that the relevant provisions of Regulation (EC) 725/2004 take precedence over those of Directive 2005/65.

8.1.4. Reviews and amendments to a PSA

The Member State concerned shall ensure that Port Security Assessments are reviewed, as appropriate, **at least once every five years** and whenever there are changes within the port.

It is **important** to recall that:

- In any case, even if the implementation of the provisions of article 2.4 of Directive 2005/65/EC is envisaged, a Port Security assessment remains mandatory, as well as its periodical revision at least every 5 years;
- PSAs shall be reviewed following the approval of any new Port Facility Security Assessments within the port[81].

It is **recommended** that:

- The review of PSAs is not to be outlined in a separate document, but it should be integrated in the main text of the original assessment, in order to make the text easily readable.
- PSAs should be provided with a Record of changes in which each amendment to the assessment should be registered.

[81], Dir.2005/65/EC Art.6.1

- The revision of the PSA should start well in advance (i.e.4 to 6 months) before the expiration date of the current PSA. This would avoid that the PSA expires at the 5 years anniversary date without concluding the revision of new PSA and its formal approval.

It is a **good practice** that ✓

- Member States request that the concerned Port Authority/ Designated Authority/ RSO conduct an annual update of the PSA. This annual update can allow the swift inclusion in the PSA of the latest port physical and structural modifications (if any), and to update the list of port facilities or the PFSO contacts if required. A similar approach can then be put in place for PSPs.

8.2. Port Security Plan (PSP)

The Port Security Authority – which might also be the "competent authority for maritime security" provided for under Regulation (EC) No 725/2004 as designated by the Member State[82] - shall be responsible for the preparation and implementation of Port Security Plans based on the findings of Port Security Assessments.

8.2.1. Content and Approval

The Port Security Plan sets out the practical details of the security measures. It will be based on the findings of the Port Security Assessment. It shall adequately address the specificities of the different sections of a port and shall integrate the security plans of all port facilities established pursuant to Regulation (EC) No 725/2004 within the boundaries of the ports. Information gathered through PSAs, actions to be undertaken under each security level, identification of stakeholders, measures, procedures and actions that must be consistent with the perceived risk and may vary, depending on the security level and between port areas, training and exercises and what to do in the event of a threat or an actual event shall be included.

For some areas, access control or security requirements should enter into force only at security level 2 or 3. Many areas can be totally open according to the port access requirements or port layout as being urban areas or public infrastructures and therefore they may not need to be closed or controlled at security level 1or even 2.

Port Security Plans shall be approved by the Member State concerned before their implementation.

[82], Dir. 2005/65/EC Art.5.3

It is **important** to recall that:

- PSPs address all the requirements provided in Annex II of the Directive;
- PSPs take into account the conclusions of the Port Security Assessments, including the countermeasures identified to reduce vulnerabilities and weaknesses and that those are fully implemented.
- A PSP is not required when the provisions of article 2.4 of Directive 2005/65/EC in the port;. In order to this provisions, the PSA should conclude that the limits of the Port and Port Facility are the same in which case only a PFSP would be required.;
- The PSP should assign tasks and specifies work plans and procedures in the following areas:
  - Access requirements: for some areas, these requirements only come into effect if security levels exceed a certain limit. All requirements and limits must be detailed in the port security plan;
  - Requirements for checking identity documents, baggage and goods: the requirements can only be applied in certain areas and be fully applicable only in some of them.
- The approvals of the PSPs are substantiated in an appropriate document (letter of approval or a signed and dated copy of the Port Security Plan)

It is **recommended** that:

- PSPs shall be approved by the Member State concerned within a reasonable timeframe after the approval of the Port Security Assessments (maximum 3 months).
- PSPs describe and detail the working instructions and/or security operational procedures (SOPs) necessary for the correct implementation of the security activities in the ports. In the case where such elements are not integrated in the PSP as approved, it has to be ensured that related references are made in the Port Security Plan;
- If a private company is assigned to perform specific security duties in the port (i.e. port security guards), a related service agreement shall detail the tasks to be performed in relation with the parts of the PSP that they are supposed to fulfil.
- In order to reduce the administrative workload, when 2 or more ports lie in the same geographical area, and their separation is not physical but it can be considered purely artificial, a unique Port Authority can be made responsible for those ports when public infrastructures and services are common. In such case, a single and combined PSA and PSP should be drafted and approved as an overarching document encompassing all the requirements of Annexes I and II of the Directive

8.2.2. Reviews and amendments to a PSP

The Member State concerned shall ensure that Port Security Plans are reviewed, as appropriate, **at least once every five years** and whenever there are changes in the port or following the review of the PSA.

It is **important** to recall that:

- PSPs are maintained on the basis of the last approved PSAs.

👍 It is **recommended** that:

- PSPs should include a Record of changes in which each amendment to the plan should be registered. PSPs should be modified whenever required at any time during the five years of validity. In any case modifications and the required reapproval should be conducted when significant changes occur in a port, such as there are new port facility operators, major port works that have an impact on the security of the port or when for example new policies and procedures regarding access control, monitoring of port areas or changes of port road traffic flows are taking place.
- The PSA provides a static picture of the security of the port at a given time. The PSP must be based on the PSA in such a way that the measures determined in the PSP address the issues found in that picture. Considering this, there should be a timely link between the PSA and the subsequent PSP. Consequently, it would be advisable that the time span between the adoption of a PSA and the drafting or revision of the PSP does not exceed 6 months

The review of a PSP should start well in advance (i.e.4 to 6 months) before the expiration of the current PSP. This would avoid that the PSP expires at the 5 years anniversary date without concluding the revision of new PSP and its formal approval

8.3. Port Security Officer

A Port security officer is the person tasked to manage and coordinate security in the port, fulfilling the role of point of contact for port security related issues. His/her designation shall be approved by the Member State concerned for each port. Where practicable, each port shall have a different port security officer. However, if deemed appropriate, a PSO may be shared between several ports.

It is **important** to recall that:

- A close cooperation between the PSO and the PFSOs shall be ensured. Periodical coordination meetings should be organised to discuss the security related issues in the port and their implementation in accordance with the provisions of the Port Security Plan.
- All port security incidents should also be reported to the port security officer and duly recorded.
- The PSO should be nominated (letter of nomination or other written evidence) by the competent authority for maritime security of the Member State.

👍 It is **recommended** that:

- A PSOs might be approved for more than one port, however the approval process by the Member State should also take into account the practicality of this appointment (e.g. geographical location, workload, typology, …).
- Unless the provisions of article 2.4 of Directive 2005/65/EC apply, the appointment of a PSO also as PFSO of port facilities comprised in same port might be in compliance with the legislation however, it is not recommended due to potential lack of efficiency due to the work overload if appointed for more than one PF.
- Any PSO is provided with the necessary authority /powers in order to fulfil the tasks provided for to this function by Directive 2005/65/EC.

8.4. Qualifications and trainings

There are no training obligations for Port Security Officers. However, courses for Port Facility Security Officers (PFSO) cover the knowledge required for a PSO for a large part. Therefore, it is recommended that the persons to be appointed as PSO should at least be trained and qualified as PFSO (*IMO Model Course 3.21*).

Member States should define the procedures aimed at training, education and familiarization for PSOs depending on their own internal organisations and rules.

It is a **good practice** that ✓

- Cybersecurity training at different levels is considered as part of the security training programme in order to create a cybersecurity culture across the organisation.
- Introducing the figure of the Chief Information Security Officer (CISO) in the organisation to ensure that cybersecurity threats are considered, adequate preparedness measures are taken, and suitable response and recovery procedures can be implemented if necessary.

8.5. Training exercises

Security awareness is vital to the safety, security and health of port personnel and others working in the port, who should be made aware of their responsibilities to fellow workers, the port community and the environment.

Appropriate training of personnel working in the port should maximize personal awareness of suspicious behaviour, incidents, etc.

Various types of training exercises which may involve participation of port facility security officers, in conjunction with the relevant authorities of Member States, company security officers, or ship security officers, if available, to check that the PSP remains current and achievable by identifying changes that may impact on any critical response, resource or consequence factor.

These training exercises may be:

- (1) full scale or live;
- (2) tabletop simulation or seminar; or
- (3) combined with other exercises held such as emergency response or other port State authority exercises.

It is **important** to recall that:

- Training requirements described in the PSP shall ensure that the port security personnel are proficient in all assigned security duties, focused on particular roles and tasks in the port or at external facilities serving the port. Large-scale exercises are crucial for training and testing the coordination between the various components of the PSP;
- Exercises **shall be carried out at least once each calendar year** with no more than 18 months elapsing between the training exercises;
- The Port Security Authority considers the necessity to diversify the types of exercise in order to properly test communication, coordination, resource availability and response in accordance with the elements contained in the PSP, avoiding the recourse to repetitive and / or not sufficiently realistic scenarios

It is **recommended** that:

- Exercises are evaluated in order to verify the effectiveness and functionality of the PSPs. After the completion of each exercise, a debriefing should be organised with all participants in order to evaluate the overall and individual performance, streamline communication and organisation, weaknesses and possible improvement. The minutes of such meetings should be retained and recorded;
- When carried out in combination with other exercises held by other authorities, it has to be ensured that the structure of the document, when prepared by said authorities, provides also the engagement of the security related issues contained in the PSP, without giving effect to scenarios in which the element of maritime security is poorly developed;
- Written evidence of the participation of the port security personnel involved in the exercises should be retained and recorded in order to attest their activity in the training;

- Although each port is different, and each situation demands its own particular approach, Member States, through their competent authorities, should encourage, for obtaining guidance and inspiration, to consult the "*Exercitium - European handbook of maritime security **exercises** and drills*"

It is a **good practice** that ✓

- Cybersecurity drills and exercises are considered as part of the security exercise and training programme.

8.6. Records

Records of the security activities outlined in the PSP are considered essential to provide evidence of compliance with the requirements of the Directive.

8.7. Inspections and controls of ports

Member States shall set up a system ensuring adequate and regular supervision of the port security plans, their implementation and conformity checking[83]. The monitoring shall be coordinated with other control activities carried out in the port.

A regular supervision has to be periodically conducted by the competent authorities/designated authorities of the Member States in order to verify that appropriate measures and procedures are properly implemented as detailed in the Port Security Plans and to take adequate remedial action in case of failures.

The inspection activity related to the application of the measures and procedures established in the Port Security Plans is the cornerstone on which port security founds. Member States shall establish how to ensure and test its effectiveness.

It is **important** to recall that:

- Member States shall set a minimum number of inspections in each port to be undertaken for the supervision of the implementation of Port Security Plans within their five-year validity period. The services of the European Commission recommend inspections at least once every year.
- Whenever practical, the above-mentioned port security Inspections should be combined at the same time with security inspections in the port facilities in order to assess that security measures taken pursuant Regulation (EC) 725/2004 benefit from enhanced port security measure detailed in the PSP.

[83] Art.7.6 and 13, Dir.2005/65/EC

👍It is **recommended** that:

- An information report on the results of the inspection should be sent by the competent authorities/designated authorities to the National Administration responsible to monitor the maritime security within an established time frame from the date of the activity. Such report should contain the following information:
  - Description of the activities carried out;
  - List of observations, accompanied by the regulatory reference;
  - Actions taken for any non-compliance identified, impositions and time frames for the rectification and conclusion of pending processes.
- Such reporting will allow the National Administration of the Member State responsible for the maritime security to adequately monitor the state of play of the ports under their jurisdiction, providing instructions and take appropriate actions.
- Member States are encouraged to make the best use of the checklist developed by the EC services (adopted with MARSEC doc 7909), fully or partially, depending on their needs, and eventually to adapt them by integrating any specific requirements contained in their applicable national maritime security legislation and rules.

  Such checklist should facilitate inspections by the authorities of the compliance with the applicable legislation by the ports and, at the same time, it could be used as a guide for self-verifications by the operators

8.8. Delegation of tasks to RSOs on port security

Member States may appoint recognised security organisations (RSOs) for the purposes specified in the Directive. RSOs have to hold appropriate expertise in security matters and appropriated knowledge in port operations before being authorised to carry out port security assessments and to draft plans. RSOs shall fulfil the requirements set out in Annex IV of the Directive.

A RSO which has made a port security assessment or review of such an assessment for a port is not allowed to establish or review the port security plan for the same port.

However, a RSO which has made a port security assessment or port security plan is allowed to draft port facility security assessments and subsequently the port facility security plans of port facilities within the same port. In fact, there is no contradiction between the two legal instruments (Port Directive 65/2005 and Regulation (EC) 725/2004) in terms of using RSOs for different security related tasks/ drafting of documents of Ports or Port Facilities.

As follows some case scenarios to help to understand in which cases the same RSO can be used for providing and undertaking certain port /port facility security related activities:

1. If one RSO (n°1) drafts the PSA for the Port Directive of a given port under Art.2.4 future arrangements and another RSO (n°2) drafts the PFSA for the single port facility in that port, could RSO (n°1) draft the PFSP of that single port facility? Yes, it possible.

2. One RSO made the port assessment under article 2.4, the same RSO might conduct the PFSA of the port facility under Regulation (EC) 725/2004 and also the same RSO can draft subsequently the PFSP of the same port facility.
3. One port has several port facilities. The port facility security plans are drafted by different RSOs. Any of those RSOs might draft the required PSA under the Port Directive.
4. The same case scenario as above. One RSO might draft the PSP of a given port, despite the fact that the RSO has drafted the PFSA and subsequently the PFSP of a port facility of that port.

8.8.1. Authorisation of RSOs

Before authorising a Recognised Security Organisation, Member States shall verify the conditions to be fulfilled by a recognised security organisation in accordance with Annex IV of the Directive. Targeted audits in the RSO shall be conducted to ascertain that such conditions are in place and maintained.

It is **important** to recall that:

- Security consultants cannot draw up port security assessments and port security plans if not appointed by the Member State as RSOs fulfilling the conditions set out in Annex IV.

It is **recommended** that:

- The appointments by the Member States are in the form of an agreement between the parties, including the details of the tasks to be delegated to the RSO, i.e. the scope of carrying out Port Security Assessments and/or Plans, reporting procedures, etc.
- The general conditions and terms of an agreement should be clearly provided for in the written document, if required, in view of allowing the parties to understand and perform their obligations and responsibilities. Access to the internal instructions, circulars and guidelines for port security of the National Maritime Administration should be made available to the RSO concerned. Imprecise clauses of the agreement may result into a poor performance of the agreement by the parties.

8.8.2. Monitoring and controls of RSOs by Member States

Member States shall monitor the activity of RSOs, that is limited to the preparation of the PSAs and/or PSPs for the ports, as well as PFSAs and PFSPs for the port facilities as a way of ensuring consistency in their approach and their quality of work through periodical audits, in order to ensure that the international and national legal obligations, national maritime security instructions and procedure are fully complied with.

9. Enforcement of penalties

As for Regulation 725/2004, the implementation of maritime security in ports needs a national legislative and jurisdictional support.

It is **important** for Member States to:

- Ensure that effective, proportionate and dissuasive penalties are introduced for infringements of the national provisions adopted pursuant to the Directive. Their national legislation shall include an enforcement regime accompanied by meaningful penalties (Article 17).

It is **recommended** that:

- The national competent authorities responsible for the enforcement of Article 17 of the Directive clearly assign this activity to the officers in charge of exercising it;
- Irrespective of the ultimate sanctions available to a national authority of the introduced penalties, Member States take a stepped approach when seeking to ensure that an identified security deficiency in the port is corrected. In case there is a need for a more robust approach, that might warrant officers in charge of conformity check to take action in their capacity, such officers should act in an effective, proportionate and dissuasive way for which they need to be properly empowered and trained.

10. Communication of information

Member States need to communicate to the IMO and to the Commission, information related to[84]:

- National authority names and contact details;
- RSO names and contact details;
- Alternative Security Arrangements;
- Equivalent Security Arrangements.

[84] Reg. 725/2004 Annex I reg. 13

For easy reference, Table 1 below indicates the communication requirements for Member States.

Table 1. Communication of Information to the EC

Regulation (EC) No 725/2004 on enhancing ship and port facility security	*Article 4.1 of Regulation (EC) 725/2004*	*Under SOLAS XI-2 Reg 13.1*	*13.1.1*	*National Authorities*
			13.1.2	*List of Port Facilities*
			13.1.3	*Receive and handle SSAS*
			13.1.4	*Communication from Contracting Governments*
			13.1.5	*Advice to ships*
		Under SOLAS XI-2 Reg 13.2, 3, 4, 5 & 6	*13.2*	*RSOs*
			13.3	*List of PFSPs*
			13.4	*Revised & updated list of PFSPs*
	Article 5.2 of Regulation (EC) 725/2004		*13.5*	*Alternative. Sec. Arrangements*
			13.6	*Equivalent. Sec. Arrangements*
	Regulation (EC) 725/2004		*Article 4.3*	*Occasional. Port Facilities & Info*
			Article 9.2	*Focal Point*
	Other required notifications under Regulation (EC) 725/2004		*Article 4.2*	*ISPS B/4.16*
			Article 9.3	*National Programme*
			Article 9.4	*Annual Monitoring Reports*
			Article7.4	*Exemption of the provision of prearrival information*[85]
	Regulation (EC) 725/2004		*Article 3.2*	*Class A Ships and Port Facilities*
			Article 3.3	*Other ships & Port Facilities*
Directive 2005/65/EC on enhancing port security			*Article 18*	*National legislation*
			Article 12	*Focal point*
			Article 12	*List of ports*

It is **important** to recall that:

- Member States are obliged to communicate all information required by SOLAS XI-2 to the IMO (GISIS database) and to keep it updated continuously as necessary[86].

It is **recommended** that:

- Due diligence be applied to ensure availability and correctness of public information, keeping in mind that such information as is made available on open platforms such as IMO GISIS is meaningfully used for operational reasons by various stakeholders.

[85] Communication of the lists of exempted companies and ships under the provisions of Article 7 (4) of Regulation (EC) No 725/2004: Table under Doc. 4107 Rev. should be used as agreed at MARSEC-42

[86] Reg. 725/2004 Annex I reg. 13 and MSC.1/Circ.1603

11. Monitoring Reports

Member States are required to provide to the Commission annual reports of their activity in respect of maritime security, including, *inter alia*, data on the inspections they carried out, the number of officers available. Member States should put in place a system to collect this data[87].

👍It is **recommended** that:

- Member States, when putting in place a system for collecting data related to the Monitoring Reports, ensure that said system be as elaborated as possible to give Member States a view as comprehensive as possible of their maritime security activity. This could possibly include the development of performance indicators that could help to better assess said activity.

[87] Reg. 725/2004 9.4, minutes of the 17th MARSEC meeting point 8.1 and MARSEC doc 1707

Appendix A. References

No.	Doc.	Remarks
1	Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security	
2	Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security	
3	Commission Regulation (EC) No.324/2008 on procedures for conducting Commission inspections in the field of maritime security	
4	Directive 2009/21/EC of the European Parliament and of the Council of 23 April 2009 on compliance with flag State requirements	
5	Directive 2009/15/EC of the European Parliament and of the Council of 23 April 2009 on common rules and standards for ship inspection and survey organisations and for the relevant activities of maritime administrations	
6	Directive 2009/16/EC of the European Parliament and of the Council of 23 April 2009 on port State control	
7	Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC	
8	Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC	
9	Commission Implementing Regulation (EU) 2018/773 of 15 May 2018 on design, construction and performance requirements and testing standards for marine equipment and repealing Implementing Regulation (EU) 2017/306	
10	Regulation (EC) No 391/2009 of the European Parliament and of the Council of 23 April 2009 on common rules and standards for ship inspection and survey organisations	
11	The following extracts of SOLAS 1974 (consolidated version): Chapter XI-2 (Special Measures to Enhance Maritime Security): all the text in one file, and all its regulations in separate files, Chapter I/2 (Definitions), Chapter I/ 6 (Inspection and Survey) Chapter I/19 (on Control by port States) Chapter V/19 and 19-1 (on Automatic Identification System (AIS) and long-range identification and tracking, (LRIT) Chapter IX/1 (definitions) Chapter XI-1/3 (on Ship's identification number, SIN) Chapter XI-1/5 (on Continuous Synopsis Record, CSR) Chapter XI-2 Chapter XIII Verification of Compliance	
12	International Ship and Port Facility Security Code (ISPS Code).	
13	SOLAS/Conf.5 Res.2 amended by MSC 196 (80) International Ship and Port Facility Security Code (the ISPS Code), as amended	Non-mandatory

14	A.917(22), as amended by IMO Res. A.956(23): Guidelines for the on-board operational use of shipborne Automatic Identification Systems (AIS).	Non-mandatory
15	A.959 (23) Format and guidelines for the maintenance of the continuous synopsis record (CSR) as amended by MSC.198(80)	
16	A.1047 (27) Principles of minimum safe manning	Non-mandatory
17	A.1070(28) IMO Instruments Implementation Code (III CODE)	
18	A.1117(30) on IMO ship number scheme;	Non-mandatory
19	MSC.136 (76) Performance Standards of Ship Security Alert System	Non-mandatory
20	MSC.147 (77) Adoption of the revised performance standards for a ship security alert system	Non-mandatory
21	MSC.159(78) on Interim guidance on control and compliance measures to enhance maritime security.	Non-mandatory
22	MSC.349 (92) The Code for Recognized Organizations (RO Code)	
23	MSC/Circ. 1072 Guidance on provision of ship security alert systems	Non-mandatory
24	MSC/Circ. 1074 Measures to enhance maritime security: Interim guidelines for the authorization of Recognized Security Organizations acting on behalf of the Administration and/or Designated Authority of a Contracting Government	Non-mandatory
25	MSC/Circ. 1109/Rev.1 False security alerts and distress/security double alerts	Non-mandatory
26	MSC/Circ.1111 of 7 June 2004: Guidance relating to the implementation of SOLAS Chapter XI-2 AND the ISPS Code	Non-mandatory
27	MSC/Circ.1113: Guidance to port State control officers on the non-security related elements of the 2002 SOLAS amendments	Non-mandatory
28	MSC/Circ.1130: Guidance to masters, companies and duly authorised officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port	Non-mandatory
29	MSC/Circ.1155 Guidance on the message priority and testing of ship security alert systems	Non-mandatory
30	MSC/Circ.1190 Guidance on the provision of information for identifying ships when transmitting ship security alerts	Non-mandatory
31	MSC.1/Circ.1192 Guidance on voluntary self-assessment by SOLAS Contracting Governments and port facilities	Non-mandatory
32	MSC.1/Circ.1193 Guidance on voluntary self-assessment by Administrations and for ship security	Non-mandatory
33	MSC-FAL.1/Circ. 3 Guidelines on Maritime Cyber Risk Management	Non-mandatory
34	FAL 5./Circ. 39/Rev.2	Non-mandatory