



## GUIDELINES FOR SHIPPING COMPANIES

### DEVELOPMENT AND IMPLEMENTATION OF A METHODOLOGY FOR THE PERFORMANCE OF A SHIP SECURITY ASSESSMENT

(in compliance with the International Ship and Port Facility Security (ISPS) Code)

## Content:

<b>A. General</b>	<b>3</b>
1. Scope of application	3
2. Objective	3
3. Requirements for shipping companies	3
4. Definitions	4
5. References	5
<b>B. Ship Security Assessment (SSA)</b>	<b>6</b>
1. Purpose	6
2. Responsibilities	6
2.1 Company Responsibility	6
2.2 The Company Security Officer (CSO)	7
2.3 The Ship Security Officer (SSO)	8
3. SSA Requirements	8
3.1 On-scene security survey	8
3.2 Documentation	9
3.3 Independence of assessment and approval activities	9
3.4 Approval of SSP and SSA documentation	9
3.5 Language requirements	9
3.6 Training for ship security	10
3.7 Implementation, verification, certification	11
4. SSA Performance	12
4.1 Assessment planning	12
4.1.1 Review of information	12
4.1.2 Elements to be considered	12
4.1.3 Expert assistance	13
4.1.4 Information to be obtained and recorded by the CSO	14
4.2 Performance	15
4.2.1 On-scene security survey	15
4.2.2 Access to the ship	16
4.2.3 Determination of existing security measures and guidance	16
4.2.4 Protection priorities	17
4.2.5 Identification of possible threats	18
4.2.6 Consideration of conflicts	19
4.2.7 The effect of security measures on ship's personnel	19
4.2.8 Reporting	19
4.3 Follow up	20
4.3.1 Periodic Review of the SSA.	20
<b>Appendix 1: Step by step approach</b>	<b>21</b>
<b>Appendix 2: Sample worksheet 1</b>	<b>24</b>
<b>Appendix 3: Sample worksheet 2</b>	<b>26</b>
<b>Appendix 4: Sample worksheet 3</b>	<b>30</b>
<b>Appendix 5: Sample worksheet 4</b>	<b>36</b>
<b>Appendix 6: Sample SSA Report</b>	<b>44</b>

## General

### 1. Scope of application

These guidelines apply to the performance of security assessments on ships in accordance with the International Ship and Port Facility Security (ISPS) Code.

***Additional GL Guidance:***

*SOLAS XI-2 Regulation 2 specifies that the following types of ships engaged on international voyages have to comply with the requirements of the ISPS Code:*

- *passenger ships including high-speed passenger craft;*
- *cargo ships, including high-speed craft of 500 gross tonnage and upwards; and*
- *mobile offshore drilling units.*

*Reference: ISPS Code A/3.1.1*

### 2. Objective

The objective of these guidelines is to provide a working tool for the implementation of the ISPS Code requirements relevant to security assessments on ships by giving practical assistance for:

- .1 the development of procedures to conduct security assessments;
- .2 information and preparation of personnel for the performance of security assessments;
- .3 identification of documentation requirements.

The documented security assessment is an essential and integral part for developing and updating the ship security plan (SSP) and a pre-condition for its approval by the flag State administration or Recognised Security Organisation (RSO).

### 3. Requirements for shipping companies

The following requirements relevant to security assessments have to be satisfied by shipping companies:

- .1 development of a methodology for security assessments for ships operated by the Company;
- .2 development of procedures to conduct on-scene security surveys on their ships;
- .3 definition of documents and records to be kept for the performance of security assessment;
- .4 establishment of measures for re-assessment after changes in security requirements or security arrangements and resulting amendments to the SSP;
- .5 establishment, implementation and maintenance of the SSP on the basis of the security assessment.

***Additional GL Guidance:***

*The ISPS Code consists of*

- *Part A - Mandatory*
- *Part B - Recommended (GL recommends to comply with all the requirements as stipulated in Part B)*

## 4. Definitions

- .1 *International Ship and Port Facility Security (ISPS) Code* means the International Code for the Security of Ships and of Port Facilities consisting of part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization;
- .2 *Convention* means the International Convention for the Safety of Life at Sea, 1974, as amended;
- .3 *Company* means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code;
- .4 *Ship Security Assessment (SSA)* means an assessment of the security risks of the operation of a ship;
- .5 *Ship Security Plan (SSP)* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident;
- .6 *Company Security Officer (CSO)* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained, and for liaison with port facility security officers and the ship security;

### **Additional GL Guidance:**

*Although the definition of an CSO is similar to that for the "Designated Person" in the ISM Code, the word ashore is not included. This will clarify the matter with regard to instances where the master is also the owner of the vessel and there is no company infrastructure ashore. In such cases the master may be the company security officer and the ship security officer.*

- .7 *Ship Security Officer (SSO)* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers;
- .8 *Security incident* means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity;
- .9 *Security Level (SL)* means the qualification of the degree of risk that a security incident will be attempted or will occur;
- .10 *Ship/port interface* means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship;
- .11 *Ship-to-ship activity* means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another;
- .12 *Recognized Security Organization (RSO)* means an organization with appropriate expertise in security and anti-terrorism matters recognized by the Administration (or designated authority) and authorised by it to carry out assessment, verification, approval and certification required by Part A of this Code, on its behalf;
- .13 *Designated Authority* means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility;
- .14 *Contracting Government* means the Contracting Government, related to port facility security, within whose territory the port facility is located and includes a reference to the Designated Authority;
- .15 *Port facility* means a location, as determined by the Contracting Government or designated authority, where interaction takes place between a ship and a port.

## 5. References

These Guidelines are based on:

- .1 SOLAS 1974 as amended Chapter XI-2 Special measures to enhance maritime security;
- .2 International Ship and Port Facility Security (ISPS) Code Parts A and Part B;
- .3 United States Coast Guard (USCG) Navigation and Vessel Inspection Circular (NVIC) 10-02, Security Guidelines for Vessels;
- .4 British Standard (BS) 8800 Guide to Occupational Health and Safety Management Systems;
- .5 MSC/Circ.443, Measures to Prevent Unlawful Acts against Passengers and Crew on Board Ships;
- .6 MSC/Circ.623, Piracy and Armed Robbery against Ships, guidance to ship owners and ship operators, ship masters and crews on preventing and suppressing acts of piracy and armed robbery against ships;
- .7 Resolution A.922(22) Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery against Ships;
- .8 International Shipping Federation (ISF) International Chamber of Shipping (ICS) Pirates and Armed Robbers – A Master's Guide;
- .9 International Safety Management (ISM) Code.

*Additional GL Guidance:*

*SOLAS XI-2 Regulation 4*

*Requirements for companies and ships to comply with the ISPS Code part A and to take into account ISPS Code Part B which provides recommendations for the implementation of the requirements stipulated in part A. The requirements include the performance of ship security assessments (SSA).*

*SOLAS Chapter XI-2 Regulation 11; 12*

*Contracting Governments may allow alternative or equivalent security arrangements for ships flying their flag. This may have an influence on the scope of the ship security assessment.*

## B. Ship Security Assessment (SSA)

### 1. Purpose

The purpose of a SSA is to identify and analyse the security risks for a given type of ship in a trading area. The results of the security assessment provide the basis for measures which are essential to develop, implement, maintain and update the ship security plan (SSP).

*Additional GL Guidance:*

*SSA means:*

- *a judgment of the security risks identified for a given ship operation;*
- *the identification of precautions already installed (e.g. hardware) or existing security measures (e.g. training, watch keeping);*
- *determination and implementation of further measures to mitigate the risks.*

*Reference: ISPS Code Part A/1.2, 8.1*

### 2. Responsibilities

#### 2.1 Company Responsibility

The Company shall appoint

- .1 a Company Security Officer (CSO) for the Company;
- .2 a Ship Security Officer (SSO) for each ship.

*Additional GL Guidance:*

*The Company may appoint more than one CSO provided it is clearly stated in the SSP for which ship or ships each individual CSO is responsible.*

The Company must provide the necessary support to ensure that the CSO, the Master and the SSO are able to perform their duties and responsibilities in compliance with the ISPS Code.

*Additional GL Guidance:*

*Management support shall include provision of:*

- *financial and personnel resources;*
- *training;*
- *information;*
- *tools and guidance.*

*Reference: ISPS Code Part A/6.2, 11.1, 12.1; Part B/1.9, 1.10*

## 2.2 The Company Security Officer (CSO)

The CSO has to ensure that the SSA is carried out by competent persons with appropriate skills to evaluate the security of a ship, in accordance with the requirements of Part A of the ISPS Code taking into account the guidance given in Part B of the ISPS Code.

The duties and responsibilities of the CSO related to the SSA include, but are not limited to:

- .1 advising what threats may be encountered by the vessel, using appropriate security assessments and other relevant information;
- .2 ensuring that the initial SSA and the periodic reviews of the assessments are carried out;
- .3 ensuring the development and maintenance of the SSP;
- .4 modifying the SSP to correct deficiencies and satisfy the security requirements of the individual vessel;
- .5 enhancing security awareness and vigilance;
- .6 ensuring adequate training for personnel responsible for the security of the vessel;
- .7 coordinating implementation of the SSP with the SSO and the relevant designated representative on behalf of the port or PFSO;
- .8 coordinating and ensuring consistency between security requirements and safety requirements;
- .9 ensuring that, if sister ship or fleet security plans are used, the plan for each vessel accurately reflects the vessel-specific information and;
- .10 ensuring that any alternative or equivalent arrangements approved for a particular vessel or group of vessels are implemented and maintained.

***Additional GL Guidance:***

- *the CSO needs not personally perform the SSA, but the ultimate responsibility for the correct assessment performance rests with him (see para. 3.6, Training);*
- *the CSO should clarify the port security level(s) with the Port Facility Security Officer (PFSO) or other relevant parties (e.g. local agent, designated authority) in due time before the ship's ETA.*

*Reference: ISPS Code Part A/8.1, 8.2, 11, 13; Part B/8.1*

## 2.3 The Ship Security Officer (SSO)

The duties and responsibilities of the SSO related to the SSA include, but are not limited to:

- .1 regular security inspections of the vessel;
- .2 implementing, maintaining, and monitoring the SSP;
- .3 proposing modifications to the SSP;
- .4 enhancing security awareness and vigilance on board;
- .5 ensuring that adequate training has been provided to vessel personnel;
- .6 coordinating implementation of the SSP with the CSO and the relevant designated representative on behalf of the port facility;
- .7 ensuring that security equipment onboard the vessel or associated with vessel security is properly operated, tested, calibrated and maintained; and reviewing and completing a Declaration of Security agreement.

***Additional GL Guidance:***

*The SSO should, in respect of the SSA, have the following responsibilities:*

- *assist the CSO in the performance of security assessment(s) including on-scene security survey(s) on the ship(s);*
- *propose modifications to the SSP which may require a new SSA.*

*Reference: ISPS Code Part A/12.2, 13.2*

## 3. SSA Requirements

### 3.1 On-scene security survey

A SSA must include an on-scene (i.e. on board) security survey covering, as a minimum, the security aspects specified in 4.2.1 and the following:

- .1 identification of existing security measures, procedures and operations;
- .2 identification and evaluation of key ship board operations and their relevance to security risks and their importance to be protected;
- .3 identification of possible threats to the key ship board operations, the likelihood of their occurrence and the consequences if they occur, in order to establish and prioritize security measures;
- .4 identification of weaknesses, including human factors in the infrastructure, policies and procedures; and
- .5 identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing the ship's vulnerability.

***Additional GL Guidance:***

*It is generally agreed that "risk-based decision-making" is one of the best tools to complete a security assessment and to determine appropriate security measures for a vessel.*

*"Risk-based decision-making" is the tool to:*

- *a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function;*
- *identify actions to reduce the vulnerability and mitigate the consequences of a security breach.*

*Reference: ISPS Code Part A/8.4*



## 3.2 Documentation

The SSA must be:

- .1 documented by the assessor;
- .2 reviewed, accepted and retained by Company management.

***Additional GL Guidance:***

*If the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO.*

*Reference: ISPS Code Part A/8.5*

## 3.3 Independence of assessment and approval activities

The CSO must ensure that the RSO undertaking the review and approval of a SSP has not been involved in the preparation or performance of the SSA, the SSP or in the amendment procedure.

*Reference: ISPS Code Part A/9.2; 9.2.1*

## 3.4 Approval of SSP and SSA documentation

The SSP has to be developed on the basis of the results of the SSA. The SSP, or amendments thereto, and the documentation of the SSA or amendments, on which basis the plan has been developed, have to be submitted to the flag State administration or to the RSO for approval.

***Additional GL Guidance:***

*Although there is no formal requirement for the SSA to be approved, it must accompany the SSP when the SSP is submitted for approval. The approval process for the SSP should include an evaluation of the SSA to verify that it is appropriate for the ship and that all the mandatory requirements for the SSA have been fulfilled.*

*Reference: ISPS Code Part A/9.3*

## 3.5 Language requirements

The SSP must be written in the working language or languages of the ship. If the working language used is not English, French or Spanish, a translation into one of these languages is required to be included. The same applies to the SSA documentation.

***Additional GL Guidance:***

*A translation should be certified true in order to facilitate PSC inspections.*

*Reference: ISPS Code Part A/9.4*

### 3.6 Training for ship security

To fulfill their duties and responsibilities the CSO and SSO shall have knowledge and have received training in the following subjects, as appropriate:

- .1 security administration;
- .2 relevant international conventions, codes and recommendations;
- .3 relevant Government legislation and regulations;
- .4 responsibilities and functions of other security organizations;
- .5 methodology of SSA;
- .6 methods of ship security surveys and inspections;
- .7 ship and port operations and conditions
- .8 ship and port facility security measures;
- .9 emergency preparedness and response; contingency planning;
- .10 instruction techniques for security training and education, including security measures and procedures;
- .11 handling of sensitive security related information and security related communications;
- .12 knowledge of current security threats and patterns;
- .13 recognition and detection of weapons, dangerous substances and devices;
- .14 recognition, on a non discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
- .15 techniques used to circumvent security measures;
- .16 security equipment and systems and their operational limitations;
- .17 methods of conducting audits, inspection, control and monitoring;
- .18 methods of physical searches and non-intrusive inspections;
- .19 security drills and exercises, including drills and exercises with port facilities; and
- .20 assessment of security drills and exercises.

***Additional GL Guidance:***

*The Company has to ensure appropriate training to cover deficiencies in or update the required knowledge for:*

- CSO, SSO, shore-based personnel engaged in security duties;
- crew members involved in security duties and other crewmembers.

*Unless not required otherwise by the flag State administration or national or international requirements, security knowledge might be attained by:*

- participation in appropriate training courses or seminars, or
- participation in a company training program (e.g. in service training)

*Reference: ISPS Code Part A/13.1, 13.2, 13.3*

### 3.7 Implementation, verification, certification

The security measures specified in the SSP must be implemented, i.e. in operation, prior to the verification conducted by an RSO or flag State administration.

Initial verification of compliance with the ISPS Code and issuance of the International Ship Security Certificate (ISSC) is dependent on the effective implementation of the SSP and the absence of non-compliances.

***Additional GL Guidance:***

*Prior to initial verification for certification by an RSO or flag State administration, an internal security system verification (internal audit) is recommended to ensure its effective operation.*

*Reference: ISPS Code Part A/19; Part B/9.6*

## 4. SSA Performance

### 4.1 Assessment planning

#### 4.1.1 Review of information

Prior to commencement of the SSA the CSO shall collect and review all available information including:

- .1 threats for the ports the ship is calling at and the possible impact on the security of the ship and crew;
- .2 port facilities and protective measures available;
- .3 specific security guidance offered by the Contracting Governments;
- .4 any security needs and security reports;
- .5 all the information required by 4.1.4;
- .6 where feasible the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment.

*Additional GL Guidance:*

*Sources for information are, inter alia:*

- *port and flag State administrations;*
- *Recognized Security Organizations (RSO);*
- *port authorities;*
- *agents, charterers;*
- *publications such as Lloyds List, IMO News;*
- *International Chamber of Shipping (ICS);*
- *maritime associations and societies;*
- *data provided on web-sites (e.g. national travel advisories, P&I clubs, USCG);*
- *incident reports;*
- *information from Masters.*

*Reference: ISPS Code Part B/8.2*

#### 4.1.2 Elements to be considered

A SSA should address the following elements on board or of the ship itself:

- .1 physical security;
- .2 structural integrity;
- .3 personnel protection systems;
- .4 procedural policies;
- .5 radio and telecommunication systems, including computer systems and networks;
- .6 other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations on board the ship or within a port facility.

*Additional GL Guidance:*

A security assessment is a process that identifies:

- weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach;
- options to eliminate or mitigate those weaknesses identified.

*Example:*

A security assessment might reveal unprotected access points such as the pilot boarding ladder not being raised or side ports not being secured or monitored after loading stores. To mitigate this threat the following measures could be implemented:

Procedures to ensure that such access points are secured and verified by some means.

Another security enhancement may be to place locking mechanisms and/or wire mesh on doors and windows that provide access to restricted areas to prevent unauthorized personnel from entering such areas. Such assessments can identify vulnerabilities in vessel operations, personnel security, and physical and technical security.

*Reference: ISPS Code Part B/8.3*

#### 4.1.3 Expert assistance

Those involved in a SSA should be able to draw upon expert assistance in relation to:

- .1 knowledge of current security threats and patterns;
- .2 recognition and detection of weapons, dangerous substances and devices;
- .3 recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
- .4 techniques used to circumvent security measures;
- .5 methods used to cause a security incident;
- .6 effects of explosives on ship's structures and equipment;
- .7 ship security;
- .8 ship/port interface business practices;
- .9 contingency planning, emergency preparedness and response;
- .10 physical security;
- .11 radio and telecommunications systems, including computer systems and networks;
- .12 marine engineering; and
- .13 ship and port operations

*Additional GL Guidance:*

Shipping companies have to ensure that the SSA is only conducted by persons having "appropriate expertise" to assess the security of a ship. The RSO or flag State administration, in the process of the SSP approval, might request documentary evidence of such expertise which might include a reference list, a certificate of attendance of an appropriate training course or the expert's company profile.

*Reference: ISPS Code Part B/8.4*

#### 4.1.4 Information to be obtained and recorded by the CSO

Information needed by the CSO for the performance of the SSA includes:

- .1 the general layout of the ship;
- .2 the location of areas which should have restricted access;
- .3 the location and function of each actual or potential access point to the ship;
- .4 changes in the tide which may have an impact on the vulnerability or security of the ship;
- .5 the cargo spaces and stowage arrangements;
- .6 the locations where the ship's stores and essential maintenance equipment is stored;
- .7 the locations where unaccompanied baggage is stored;
- .8 the emergency and stand-by equipment available to maintain essential services;
- .9 the number of ship's personnel, any existing security duties and any existing training requirement practices of the Company;
- .10 existing security and safety equipment for the protection of passengers and ship's personnel;
- .11 escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;
- .12 existing agreements with private security companies providing ship/waterside security services; and
- .13 existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

*Reference: ISPS Code Part B/8.5*

## 4.2 Performance

### 4.2.1 On-scene security survey

An on-scene security survey has to be carried out on each ship. The objective of the on-scene security survey is to examine and evaluate existing shipboard protective measures, procedures and operations for:

- .1 ensuring the effective implementation of all ship security duties;
- .2 monitoring restricted areas to ensure that only authorized persons have access;
- .3 controlling access to the ship, including any identification systems;
- .4 monitoring of deck areas and areas surrounding the ship;
- .5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
- .6 supervising the handling of cargo and the delivery of ship's stores; and
- .7 ensuring that ship security communication, information, and equipment are readily available.

Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

#### *Additional GL Guidance:*

*During the on-scene security survey the following should be considered:*

- *the existing duties and responsibilities of all shipboard personnel, the designation of additional security duties and its affect to the safe operation of the vessel;*
- *the existing procedures or safeguards for communications and measures necessary to maintain continuous communications at all times in the case of a security threat;*
- *the existing procedures for the assessment of safety procedures and equipment and systems and additional procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;*
- *additional procedures and practices required to protect security sensitive information held in paper or electronic format;*
- *any additional and maintenance requirements, or inclusion of security and surveillance equipment and systems, if any, into the existing maintenance programs;*
- *existing procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of or security concerns; and*
- *procedures required to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.*

*Reference: ISPS Code Part B/8.14, 9.3*

#### 4.2.2 Access to the ship

The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

***Additional GL Guidance:***

*SSA to identify all means of access to the ship with the appropriate locations where access restrictions or prohibitions should be applied. Points of access are, inter alia:*

- *access ladders;*
- *access gangways;*
- *access ramps;*
- *access doors, side scuttles, windows and ports;*
- *mooring lines and anchor chains; and*
- *cranes and hoisting gear;*
- *other access points.*

*Reference: ISPS Code Part B/8.6, 9.9*

#### 4.2.3 Determination of existing security measures and guidance

The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:

- .1 the restricted areas;
- .2 the response procedures to fire or other emergency conditions;
- .3 the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers;
- .4 the frequency and effectiveness of security patrols;
- .5 the access control systems, including identification systems;
- .6 the security communications systems and procedures;
- .7 the security doors, barriers and lighting; and
- .8 the security and surveillance equipment and systems, if any.

***Additional GL Guidance:***

*Examples of restricted areas:*

- *navigation bridge, machinery spaces of category A and other control stations;*
- *spaces containing security and surveillance equipment and systems and their controls and lighting system controls;*
- *ventilation and air-conditioning systems and other similar spaces;*
- *spaces with access to potable water tanks, pumps, or manifolds;*
- *spaces containing dangerous goods or hazardous substances;*
- *spaces containing cargo pumps and their controls;*
- *cargo spaces and spaces containing ship's stores;*
- *crew accommodation; and*
- *any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.*

*The purpose of restricted areas are to:*



- *prevent unauthorized access;*
- *protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;*
- *protect sensitive security areas within the ship; and*
- *protect cargo and ship's stores from tampering.*

*Reference ISPS Code Part B/8.7, 9.18, 9.21*

#### 4.2.4 Protection priorities

The SSA should include the persons, activities, services and operations that it is important to protect. This includes:

- .1 the ship as such;
- .2 the ship's personnel;
- .3 passengers, visitors, vendors, repair technicians, port facility personnel, etc;
- .4 the capacity to maintain safe navigation and emergency response;
- .5 the cargo, particularly dangerous goods or hazardous substances;
- .6 the ship's stores;
- .7 the ship security communication equipment and systems, if any; and
- .8 the ship's security surveillance equipment and systems, if any;
- .9 key shipboard operations required to function in an emergency.

*Reference: ISPS Code Part B/8.8*

#### 4.2.5 Identification of possible threats

The SSA should consider all possible threats, which may include the following types of security incidents:

- .1 damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
- .2 hijacking or seizure of the ship or of persons on board;
- .3 tampering with cargo, essential ship equipment or systems or ship's stores;
- .4 unauthorized access or use, including presence of stowaways;
- .5 smuggling weapons or equipment, including weapons of mass destruction;
- .6 use of the ship to carry persons intending to cause a security incident and/or their equipment;
- .7 use of the ship itself as a weapon or as a means to cause damage or destruction;
- .8 attacks from seaward whilst at berth or at anchor; and
- .9 attacks whilst at sea.

***Additional GL Guidance:***

*A vessel or company needs also to consider attack scenario(s) consisting of a potential threat to the vessel under specific circumstances. Typical types of scenarios are:*

- *Intrude and /or take control of the vessel;*
- *damage/destroy the vessel with explosives;*
- *damage/destroy the vessel through malicious operations/acts;*
- *create a hazardous or pollution incident without destroying the vessel;*
- *take hostages/kill people.*

*Examples for external attack scenarios are:*

- *moving explosives \ adjacent to vessel;*
  - *from the waterside;*
  - *on the shore side;*
  - *subsurface.*
- *ramming a stationary target;*
  - *with a vessel;*
  - *with a land-based vehicle.*
- *launching or shooting weapons from a distance.*

*Another scenario might be using the vessel as a means of transfer for:*

- *materials to be used as a weapon into/out of the country;*
- *people into/out of the country.*

*Reference ISPS Code Part B/8.9*

*Examples of possible threats:*

- intruder plants explosives;
- intruder takes control of a vessel and runs it aground or collides with something intentionally;
- intruder intentionally opens valves to release hazardous materials;
- intruder opens valves/vents to release toxic materials or releases toxic material brought along;
- intruder overrides interlocks leading to damage/destruction;
- goal of the intruder is to kill people;
  - car/truck bomb;
  - damage/destruction of the vessel;
  - shooting at a vessel using a rifle, missile, etc.

#### 4.2.6 Consideration of conflicts

The SSA should take into account all possible vulnerabilities, which may include:

- .1 conflicts between safety and security measures;
- .2 conflicts between shipboard duties and security assignments;
- .3 watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;
- .4 any identified security training deficiencies; and
- .5 any security equipment and systems, including communication systems and their maintenance.

*Reference: ISPS Code Part B/8.10*

#### 4.2.7 The effect of security measures on ship's personnel

The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to:

- .1 the convenience, comfort and personal privacy of the ship's personnel; and
- .2 their ability to maintain their effectiveness over long periods.

*Reference: ISPS Code Part B/8.11;*

*Conference Resolution 11 "Human-element-related aspects and shore leave for seafarers"*

#### 4.2.8 Reporting

Upon completion of the SSA, a report shall be prepared, consisting of

- .1 a summary of how the assessment was conducted;
- .2 a description of each vulnerability found during the assessment; and
- .3 a description of counter measures that could be used to address each vulnerability.

The report shall be protected from unauthorized access or disclosure.

If the SSA has not been carried out by the Company the SSA documentation shall be reviewed and verified by the CSO.

*Reference: ISPS Code Part B/8.12, 8.13*

*Additional GL Guidance:*

*Documentation to be established during the performance of the SSA may consist of the following records:*

- *a list of threat motives for the operational parameters for that type of vessel;*
- *a list of systems, physical areas, and personnel that may be targeted and used in security incidents;*
- *a list of existing security measures related to critical operations, areas, systems, and personnel;*
- *a list of security incident scenarios or threats relevant for the operation of the ship;*
- *a list of potential security incidents assessed and prioritised;*
- *a questionnaire to perform the initial On-Scene Security Survey;*
- *a list of proposals for the improvement of vessel's security;*
- *a SSA Report with a summary of how the SSA was performed, a description of each vulnerability found during the assessment and a description of the counter measures that could be used to mitigate each vulnerability.*

#### 4.3 Follow up

In the case of changes of the operational or physical parameters of the vessel(s), the SSA with the on-scene security survey shall be repeated.

##### 4.3.1 Periodic Review of the SSA.

The SSA shall be reviewed periodically. Records of the reviews shall be prepared and kept on board for verification.

*Additional GL Guidance:*

*The SSA should be reviewed at least once every 12 months. In addition, should it be identified during training, drills, or following an incident that the SSA, and hence the SSP, are inappropriate, they should be reviewed and amended accordingly.*

*Reference: ISPS Code Part A/10.1.7*

## Appendix 1: Step by step approach

The SSA is an essential and integral part of the process of establishing, implementing, maintaining and updating the Ship Security Plan (SSP). In order to enable shipping companies to conduct such task in an organized and convenient manner, GL has developed, as a sample, a Security Assessment Report including a "STEP BY STEP APPROACH FOR THE PERFORMANCE OF A SHIP SECURITY ASSESSMENT" and associated worksheets.

The objective of the "STEP BY STEP APPROACH" is to provide a working tool for the implementation of the ISPS Code requirements relevant for the performance of a SSA including an On-Scene Security Survey and subsequent reporting.

Steps	Reference	Items to be assessed	What actions	Result	Tools
1. Identify security risk parameters for the operation of the vessel.	A/8.4.3; B/8.2	What could be the motives for security incidents on my ships and which motives should be taken into consideration? <ul style="list-style-type: none"> <li>- Political</li> <li>- Symbolic</li> <li>- Economical</li> <li>- Fear</li> <li>- Others</li> </ul>	<ol style="list-style-type: none"> <li>1. Establish worksheet</li> <li>2. Seek for information available of threats for the ports at which the vessel will call and for the area of trading</li> <li>3. Identify and classify likelihood of threat motives</li> </ol>	<ul style="list-style-type: none"> <li>- A List of threat motives for the operational parameters for that type of vessel</li> <li>- <b>Input for step 4</b></li> </ul>	<b>Sample Worksheet 1</b>
2. Identify key shipboard operations, activities, and persons that are important to be protected.	A/8.4.2; B/8.3; B/8.6; B/8.8	What is critical for the operation of the vessel and what has to be protected to avoid a security incident? <ul style="list-style-type: none"> <li>- Operations</li> <li>- Systems</li> <li>- Areas</li> <li>- Personnel</li> </ul>	<ol style="list-style-type: none"> <li>1. Establish worksheet</li> <li>2. Obtain and record the information from the general layout of ship, stowage arrangement plans, areas of restricted access, etc</li> <li>3. Identify key shipboard operations and their relevance to security risks (e.g., cargo operations, bunkering, change of crew/passengers, etc.)</li> <li>4. Identify systems, areas, and personnel that may be important to be protected</li> </ol>	<ul style="list-style-type: none"> <li>- A List of systems, physical areas, and personnel that may be targeted and used in security incidents</li> <li>- <b>Input for step 3</b></li> </ul>	<b>Sample Worksheet 2</b>

Steps	Reference	Items to be assessed	What actions	Result	Tools
3. Identify security measures, procedures, operations which are in place already and identify weaknesses, including human factors in the infrastructure, policies and procedures.	A/8.4.1; A/8.4.4; B/8.5; B/8.7; (partly B/8.14)	What existing security measures, procedures and operations are implemented and maintained to prevent security incidents? <ul style="list-style-type: none"> <li>- For critical operations</li> <li>- To protect systems</li> <li>- To avoid access to areas</li> <li>- To protect personnel</li> </ul>	<ol style="list-style-type: none"> <li>1. Use the list of systems, physical areas, and personnel that may be targeted and used in security incidents (step 2)</li> <li>2. Identify security measures in place for each critical operation</li> <li>3. Prioritize those operations, systems, areas, and personnel found critical with limited/weak security measures in place</li> </ol>	<ul style="list-style-type: none"> <li>- A list of existing security measures related to critical operations, areas, systems, and personnel</li> <li>- <b>Input for step 7</b></li> </ul>	<b>Sample Worksheet 2</b>
4. Identify potential threat scenarios.	A/8.4.3; B/8.9	How can anybody attack my ship? <ul style="list-style-type: none"> <li>- Intrude and /or take control of the vessel</li> <li>- Damage/destroy the vessel with explosives</li> <li>- Damage/destroy the vessel through malicious operations/acts</li> <li>- Create a hazardous or pollution incident without destroying the vessel</li> <li>- Take hostages/kill people</li> <li>- Etc.</li> </ul>	<ol style="list-style-type: none"> <li>1. Use the list of threat motives for the operational parameters for that type of vessel (step 1)</li> <li>2. Identify possible threat scenarios taking into account the list of possible threats (B/8.9)</li> <li>3. Use the results of the assessments (steps 1-3)</li> </ol>	<ul style="list-style-type: none"> <li>- A list of relevant security incident scenarios, or threats</li> <li>- <b>Input for step 5</b></li> </ul>	<b>Sample Worksheet 3</b>
5. Assess likelihood and potential consequences of the scenarios and set priorities.	A/8.4.3; B/8.9; B/8.10	What is the likelihood of the occurrence of the potential threat scenarios identified and what are the consequences?	<ol style="list-style-type: none"> <li>1. Use the list of relevant security incident scenarios established (step 4)</li> <li>2. Determine the relevance (yes, no)</li> <li>3. Assess the consequences (moderate, high, extreme)</li> <li>4. Assess the likelihood (likely, unlikely)</li> <li>5. Prioritize threat scenarios</li> </ol>	<ul style="list-style-type: none"> <li>- A list of potential security incidents assessed and prioritized</li> <li>- <b>Input for step 6</b></li> </ul>	<b>Sample Worksheet 3</b>

Steps	Reference	Items to be assessed	What actions	Result	Tools
6. Establish an On-Scene Security Survey checklist taking into account the prioritized scenarios and the existing measures.	A/8.4; B/8; (B/8.14 in particular)	What has to be checked on board the vessel and what is the present status? <ul style="list-style-type: none"> <li>- All ship security duties;</li> <li>- Monitoring access to restricted areas;</li> <li>- Access to the ship</li> <li>- Monitoring of deck areas and areas surrounding the ship</li> <li>- Controlling the embarkation of persons</li> <li>- Handling of cargo and the delivery of ship's stores; and</li> <li>- Ship security communication, information, and equipment</li> </ul>	<ol style="list-style-type: none"> <li>1. Establish a specific worksheet questionnaire for the ship</li> <li>2. Identify operations, areas, systems, and personnel related to the threat scenarios developed in Step 5</li> <li>3. Identify any additional items to verify onboard according to your own experience</li> <li>4. Ensure consideration of items listed in B/8.14</li> <li>5. Use the list of potential security incidents assessed and prioritized (step 5)</li> </ol>	<ul style="list-style-type: none"> <li>- A worksheet questionnaire to perform the initial On-Scene Security Survey</li> </ul>	<b>Sample Worksheet 4</b>
7. Perform an On-Scene Security Survey on the ship.	A/8.4; B/8.14; B/8.10 (in particular)	What additional security measures have to be implemented and what are the weak points of the existing? <ul style="list-style-type: none"> <li>- Weak points</li> <li>- Deficiencies</li> <li>- Training needs</li> <li>- Safety conflicts</li> <li>- Manning constraints</li> <li>- Security equipment</li> </ul>	<ol style="list-style-type: none"> <li>1. Perform an On-Scene Security Survey of the ship security by using the worksheet questionnaire developed in step 6</li> <li>2. Identify and verify measures already in place and take into account the list of existing security measures related to critical operations, areas, systems, and personnel (step 3)</li> <li>3. Identify weaknesses in the system</li> <li>4. Identification additional security measures to be implemented</li> </ol>	<ul style="list-style-type: none"> <li>- Confirmation of security measures already in operation</li> <li>- A list of proposals for the improvement of vessel's security</li> </ul>	<b>Sample Worksheet 4</b>
8. Evaluate the outcome of the SSA including the On-Scene Security Survey.	A/8.4.4; B/8.3; B/8.7; B/8.8; B/8.9; B/8.14	What security improvements are required to mitigate vulnerability and eliminate weak points? <ul style="list-style-type: none"> <li>- Improvement needs</li> <li>- Remedial actions to close "security gaps"</li> </ul>	<ol style="list-style-type: none"> <li>1. Evaluate On-Scene Security Survey results</li> <li>2. Identify needs for security improvements</li> </ol>	<ul style="list-style-type: none"> <li>- A list of vulnerabilities and countermeasures</li> </ul>	<b>Sample SSA Report</b>

## Appendix 2: Sample worksheet 1

The objective is to identify possible threat motives and potential security risks for the operation of the vessel A/8.4.3 (step 1)

Operational security risks		Examples of possible scenarios	Likelihood			Comments for further consideration
			Unlikely	Probable	Likely	
<b>1. Political motives</b>						
1.1	Is your ship trading in an area with a known or perceived unstable political situation?	Countries with elections, demonstrations, civil war, riots, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.2	Is there known or perceived political (incl. religious, ideological, ethnical, nationalistic) motives related to your ship (flag, owner, crew) or trade (cargo, passengers, trade area or port)?	Cargo (e.g. weapon parts, nuclear cargo); trade area, ports, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.3	Add other relevant questions:					
<b>2. Symbolic motives</b>						
2.1	Could your ship be used as a means to harm symbolic objects of national or international importance?	Well known buildings, statues, bridges, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	Does your ship visit a port where international events take place?	Exhibitions, sports, political, etc. (Olympic Games, EXPO, World Leader Summits, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Could your ship be used as means to harm important environmental areas?	Areas for tourism, commercial exploitation of nature (fish farming, beaches, cities, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.4	Does your ship itself represent or carry a symbolic value?	Ship carries special cargo (e.g. weapons), support operations (oil to war actions, equipment to industry projects), represent attitudes at debate (cruise, natural resources, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.5	Does the visibility or the profile of your ship, company or brand give rise to concern as a motive for unlawful acts?	Because of your policy (exploitation of labour, political attitudes), the operations you are involved (natural resources, weapons, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.6	Add other relevant questions:					



<b>3. Economical damage</b>						
3.1	Does your ship carry special cargo (economical value, restricted availability)?	Plutonium, equipment for mass destruction, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Is it likely that terror related smuggling could be taking place from ports your ship is visiting?	Smuggling of people/goods (Intelligence)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.3	Is it likely that your crew can take part in or give support to terror related smuggling?	Ethnical motives and common cause	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.4	Is your ship trading in an area known for piracy?	Refer to periodic Piracy Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.5	Does your ship, cargo or passengers represent a significant risk of hijacking?	Valuable ship, cargo and passengers used for threats and bargaining demands	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.6	Add other relevant questions:					
<b>4. Damage to society / industry</b>						
4.1	Could your ship be used to damage important geographical points for trade or commercial activity?	Block ports or canal, collide with bridges or offshore installations, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	Is the trade your ship represents critical to society?	Critical equipment to industry projects (e.g. pipelines, offshore installations, etc.), or for industry production (gold, silver, silicates, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.3	Will an unlawful act against your ship or trade harm the state of the industry?	Reduced market due to reduced trust (cruise, passenger transport, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.4	Add other relevant questions:					
<b>5. Fear and others</b>						
5.1	Can the ship be used to create fear to the society?	Discharge of oil or poisoning gas, radioactive materials, chemicals, explosion of the cargo, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Add other relevant questions:					

**Note:** The result of the overall security risk review for the operation of the vessel has to be taken into account for the identification of potential threat scenarios (step 4).

### Appendix 3: Sample worksheet 2

The objective is to identify and evaluate key ship board operations, activities and persons that is important to protect A/8.4.2 (step 2) and to identify existing security measures, procedures and operations A/8.4.1 (step 3)

		Step 2		Step 3		
Operations, systems, areas and personnel important to be protected		Criticality		Security measures in place		Describe existing measures/procedures/operations/weaknesses/limitations
		Low	High	Yes	No	
<b>1. Access control - personnel, passengers, visitors</b>						
1.1	Access ladders (including Pilot Ladders)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.2	Access gangways	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.3	Access ramps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.4	Access doors, side scuttles, windows and ports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.5	Mooring ropes and anchor chains	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.6	Cranes and hosting gear	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.7	Access by ships side (freeboard)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.8	Equipment and baggage brought onboard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1.9	Unaccompanied baggage found onboard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Add other relevant items					

		Step 2		Step 3		
Operations, systems, areas and personnel important to be protected		Criticality		Security measures in place		Describe existing measures/procedures/operations/weaknesses/limitations
		Low	High	Yes	No	
<b>2. Restricted areas on the ship</b>						
2.1	Navigation bridge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	Navigational means (radio, radar, GPS, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Machinery spaces, power supplies, steering gear rooms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.4	Emergency sources of power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.5	Spaces containing cargo pumps and their controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.6	Crew accommodation;					
2.7	Galley/pantry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.8	ventilation and air-conditioning systems and other similar spaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.9	Spaces with access to potable water tanks, pumps or manifolds.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.10	Cargo spaces and spaces containing ship's stores					
2.11	Spaces containing dangerous goods or hazardous substances	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.12	Spaces containing security and surveillance equipment and systems and their controls and lighting system controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.13	Any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

		Step 2		Step 3		
Operations, systems, areas and personnel important to be protected		Criticality		Security measures in place		Describe existing measures/procedures/operations/weaknesses/limitations
		Low	High	Yes	No	
<b>3. Cargo handling</b>						
3.1	Cargo access points (hatches, ports, manifold/pipes)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Cargo storage spaces (incl. access points)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.3	Spaces containing dangerous goods or hazardous subst.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.4	Cargo handling equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Add other relevant items					
<b>4. Ship stores handling</b>						
4.1	Access points for delivery to ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	Storage spaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.3	Access points to storage spaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Add other relevant items					
<b>5. Security monitoring</b>						
5.1	Lighting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Watch system (at sea, in port, at anchorage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.3	Security guards and deck watches, including patrols	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.4	Automatic intrusion detection advice	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

		Step 2		Step 3		
Operations, systems, areas and personnel important to be protected		Criticality		Security measures in place		Describe existing measures/procedures/operations/weaknesses/limitations
		Low	High	Yes	No	
5.5	Surveillance monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.6	Security and surveillance equipment spaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.7	Locking devices, seals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Add other relevant items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>6. Safety operations</b>						
6.1	Life boats, life rafts and life belts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.2	Alarms, signals and marking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	Evacuation routes (including Marine Evacuation Systems if applicable)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.4	Fire fighting system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.5	Communication equipment and procedures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.6	Emergency Procedures (abandon ship, fire fighting, rescue, damage to hull, etc.)					
	Add other relevant items					

## Appendix 4: Sample worksheet 3

The objective is to identify possible threat scenarios to the key ship board operations and assess the likelihood of their occurrence, in order to establish and prioritise security measures A/8.4.3.

Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
<b>1. Damage to, or destruction of, the ship (bombing, arson, sabotage, vandalism)</b>									
- Conceal explosives onboard, initiate with timer or remote device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Bring explosives onboard, suicidal/high risk action	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Place explosives in cargo, initiate with timer or remote device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Attach explosives to hull, initiate with timer or remote device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Cause explosion on or alongside ship by external craft, torpedo, mine, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Force oil/gas leakage from cargo tanks or engine room fuel tanks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Set ship on fire	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Open bow, side or stern ports, cargo hatch to sink or capsize	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Drain holes to sink or capsize	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

<sup>1</sup> Note: Possible consequences x Likelihood = Priority score

Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
- Cut pipes (water intake) to change trim	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Activate pumps to change trim	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<b>2. Hijacking or seizure of the ship or of persons on board</b>									
- Crew takes control over ship - mutiny	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Passengers take control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Stowaways/boarded person (pirates) take control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Hijacking through (bomb) threat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Hijacking of crew or passengers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Unlawful detention of ship, crew or passengers by port authority or state	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<b>3. Tampering with cargo, essential ship equipment or systems or ship's stores</b>									
- Damage or immobilize critical systems like propulsion, steering gear etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Damage or immobilize emergency sources of power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Contaminate bunker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
- Damage ship systems, navigation, loading, ballast	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Input false navigational data/guidance (radar, VTS, pilot, chart)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Contaminate drinking water, food or air-conditioning	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Release gas onboard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Contaminate cargo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Destroy lifesaving equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Destroy ship interiors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<b>4. Unauthorised access or use including presence of stowaways</b>									
- Stowaways sneaking onboard, concealment in cargo/service or storage spaces (including containers)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Boarding ship at port or during voyage as "passenger" or "crew"	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Boarding ship at port or during voyage as "pilot", "supplier", "surveyor", fake castaway	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Unauthorized boarding of ship at pilot station or VTS operations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Unauthorized boarding of ship at voyage via vessel/craft/helicopter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		



Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
- Unauthorized boarding ship at voyage via shipwreck	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
<b>5. Smuggling weapons or equipment, including weapons of mass destruction</b>									
- Conceal weapons/equipment in cargo/service or storage spaces (including containers)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Conceal weapons/equipment in crews luggage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Conceal weapons/equipment in passengers luggage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Conceal weapons/equipment in ship supplies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
<b>6. Use of the ship to carry perpetrators and their personal equipment</b>									
- Stowaways sneaking onboard /concealment in cargo or service/storage spaces (including containers)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Boarding ship at port or during voyage as "passenger" or "crew"	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Boarding ship at port or during voyage as fake "pilot", "supplier", "surveyor", or similar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
-									

Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
<b>7. Use of the ship itself as a weapon or as a means to cause damage or destruction</b>									
- Crew take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Passengers take control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Stowaways/boarded person take control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Damage or immobilize critical systems like propulsion, steering etc in a critical position (near terminal etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Given a hijacked situation (item 4): Take control over ship and hit another ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Given a hijacked situation (item 4): Take control over ship and hit a land based construction / terminal / chemical plant or similar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Given a hijacked situation (item 4): Take control over ship and hit an offshore installation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Given a hijacked situation (item 4): Take control over ship and hit a rock / provoke grounding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
<b>8. Attacks from seaward</b>									
- Pirates take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Terrorists take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Possible threat scenarios	Relevant		Possible consequences			Likelihood		Priority score <sup>1</sup>	Possible protective measures for mitigation
	Yes	No	Moderate 1	High 2	Extreme 3	Likely 2	Unlikely 1		
- Vessel rammed by terrorists using explosives	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
<b>9. Attacks whilst at sea</b>									
- Pirates take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Terrorists take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Vessel rammed by terrorists using explosives	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
<b>10. Other possible scenarios</b>									
- Environmental extremists take control over ship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Labour unrest – crew complaints, strife, lack of pay leading to unrest etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Labour strife ashore leading to problems of access to vessel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- Collateral damage – caused by explosion or terrorist activities in the vicinity of the vessel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other									
-									
-									

## Appendix 5: Sample worksheet 4

The objective of the initial On-Scene Security Survey is to examine and evaluate existing shipboard protective measures, procedures and operations B/8.14.

\*Possible vulnerabilities may include:

- conflicts between safety and security measures;
- conflicts between shipboard duties and security assignments;
- watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;
- any identified security training deficiencies; and
- any security equipment and systems, including communication systems.

Initial On-Scene Security Survey Consider also worksheets 2 and 3	Yes	No	Observations (including possible vulnerabilities and consideration of personal privacy of crew)	Recommendations (to be based on the analyses of the security observations with the aim to correct any security deficiencies)
<b>1. Monitoring of deck area and areas surrounding the ship B/8.14.4</b>				
- Lighting of all deck areas and areas surrounding the ship sufficient?	<input type="checkbox"/>	<input type="checkbox"/>		
- Responsibilities defined for the maintenance of lighting devices?	<input type="checkbox"/>	<input type="checkbox"/>		
- Responsibilities and procedures for lighting defined?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are all access points to the ship lighted?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are critical and vulnerable areas lighted?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the vessel sufficiently lighted at anchorage?	<input type="checkbox"/>	<input type="checkbox"/>		
- Do lights overlap if a light fails?	<input type="checkbox"/>	<input type="checkbox"/>		

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
- Are ship's sides properly lighted?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are there sufficient spare parts (bulbs, fuses, etc.)?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there auxiliary power available?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are measures in place to monitor the deck area?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are measures in place to monitor the area surrounding the vessel?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are standing orders for watch keeping crew members available?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are security patrols scheduled for monitoring?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a routine for briefing of crew members/ watch keepers?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are there any intrusion-detection devices and/or surveillance equipment available?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other				
<b>2. Controlling access to the ship, including any identification systems B/8.14.3</b>				
- Are the portholes and windows to shore side and waterside closed and secured?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are there ladders and are they secured from unauthorized access?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are there measures to control access to all identified access points? see worksheet 2	<input type="checkbox"/>	<input type="checkbox"/>		

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
- Is there any equipment available to control access?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is a personnel identification system in use?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the identification system regular updated?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to deny access to the vessel?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure for reporting denial of access and the attempt to obtain access?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are vendors, visitors, workers, repairmen checked when boarding?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are random identity checks carried out to confirm reasons for boarding?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are visitors escorted throughout the ship at all times?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there only a single access point for all persons visiting the ship?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is a permanent gangway watch established?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are lines and anchor chains protected against intruders?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the ship/shore side controlled for access?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the ship/waterside controlled for access?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are security notices displayed at the gangway?	<input type="checkbox"/>	<input type="checkbox"/>		

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
<b>3. Controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects) B/8.14.5</b>				
- Is there a procedure to control embarkation of ship's crew/passengers?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a searching procedure for persons and baggage?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a secure area to search persons/ baggage/vehicles/?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the security notice containing that persons and their personal effects are liable to be searched?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to segregate checked persons from unchecked persons?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to segregate embarking from disembarking persons?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to handle unaccompanied baggage?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is unaccompanied baggage searched?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are searching responsibilities defined?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		
-				
-				

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
<b>4. Monitoring restricted areas to ensure that only authorized persons have access B/8.14.2</b>				
- Have restricted areas been established?	<input type="checkbox"/>	<input type="checkbox"/>		
- Have all the restricted areas established in worksheet 2 been taken into account and assessed?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a list or plan with all doors, hatches and openings available?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure for key and lock control?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the responsibility for locking defined?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the responsibility for issuing keys defined?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a log for issuing keys?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are keys signed for?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the distribution of master keys controlled?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are the keys and locks kept at a secure place?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are restricted areas adequately locked?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are the emergency exits of restricted areas locked from inside?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are the portholes and windows of the accommodations closed and secured?	<input type="checkbox"/>	<input type="checkbox"/>		



<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
- Are all hatches and their entrances secured by locks or other means?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are cargo hold entrances via cranes separately secured?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>		
<b>5. Supervising the handling of cargo and delivery of ship's store B/8.14.6</b>				
- Are measures in place for routine checks of cargo during cargo operations?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are visual and/or physical examinations performed?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are the seals checked on a random basis?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are checks carried out to ensure that cargo loaded matches with cargo documentation?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are checks carried out to prevent tampering of dangerous cargo?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is any scanning/detection equipment required?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are responsibilities for supervising defined?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure for checking ship's stores?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is the store delivery compared with the order?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are the packages checked for tampering?	<input type="checkbox"/>	<input type="checkbox"/>		

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
- Is the store on delivery immediately transferred to a secure area?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>		
<b>6. Ensuring that ship security communication, information, and equipment are readily available B/8.14.7</b>				
- Are technical security devices available? (CCTV, screening equipment, intrusion detection devices, alarms etc.)	<input type="checkbox"/>	<input type="checkbox"/>		
- Are procedures available for testing, maintenance and calibration of such equipment?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are security alarms agreed and used on board?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is a list of communication equipment available?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are internal communication systems available for security purposes?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is a secure place available for the storage of security information?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are persons identified who need to know, need to have, need to take security information?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		

<b>Initial On-Scene Security Survey</b> <b>Consider also worksheets 2 and 3</b>	<b>Yes</b>	<b>No</b>	<b>Observations</b> <b>(including possible vulnerabilities and consideration of personal privacy of crew)</b>	<b>Recommendations</b> <b>(to be based on the analyses of the security observations with the aim to correct any security deficiencies)</b>
<b>7. Ensuring performance of all ship security duties B/8.14.1</b>				
- Are duties and responsibilities defined for all personnel with security duties?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there sufficient crew to fulfill all the security duties?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are communication procedures available?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is a plan available for searching the ship (stowaways, illegal drugs, bombs)?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to establish, maintain and update an inventory of dangerous goods and their location?	<input type="checkbox"/>	<input type="checkbox"/>		
- Is there a procedure to familiarize the crew with security matters?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are drills and exercises required to ensure that crew can perform the designated security duties?	<input type="checkbox"/>	<input type="checkbox"/>		
- Are contingency plans available to respond on security breaches?	<input type="checkbox"/>	<input type="checkbox"/>		
- .....other	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		
-	<input type="checkbox"/>	<input type="checkbox"/>		

## Appendix 6: Sample SSA Report

# SHIP SECURITY ASSESSMENT (SSA) REPORT

**Confidential**

Name of ship		Gross tonnage	
GL Reg. No. / Name of class society		IMO No.	
Flag		Call Sign	
Port of registry		Type	

Date of SSA	
Date of On-Scene Security Survey	
Place of On-Scene Security Survey	
Name and signature of Assessor	

Summary on how the SSA was conducted:

Description of each vulnerability found during the assessment:

Description of the counter measures that could be used to address each above mentioned vulnerability:

Date SSA reviewed:		Name and Signature:	
Date SSA accepted:		Name and Signature:	