GUIDELINES FOR IMPLEMENTATION OF SHIP SECURITY ASSESSMENT

2004

In accordance with International Code for the Security of Ships and of Port Facilities
(ISPS Code)

CONTENTS

0 Introduction

0.1 General

Ship security means the status reached when the designated ship and personnel, cargoes, equipment and operations onboard the ship get protected to prevent from the illegal activities and acts of terrorism. The purpose of mandatory implementation of the ISPS Code, establishment, implementation, maintenance and continuous improvement of ship security management system is to enable the company and the ship to control maritime security risk and to enhance the effect.

Each ship in service engaged on international voyages will encounter the risk of maritime security threat. The extent of the risk changes with the changing of the service environment of the ship. An effective ship security management system is to have an ability of responding to the change of security threat.

It is generally agreed that risk-assessment-based decision-making is one of the best methods for completing a security assessment and is to determine appropriate security measures for a ship. ISPS Code encourages to adopt the method of risk assessment in ship security management. Ship security assessment is the basic part to develop and renew ship security plan. It is at least to include the following elements:

.1 determining the existing security measures, procedures and operations;
.2 determining and evaluating key onboard operations to be emphatically protected;
.3 determining the possibility of key onboard operations likely to be threatened and happening; and
.4 determining the vulnerabilities in basic facilities, policy and procedures, including human elements.

It is recognized that to ensure the safety of the ship in service is the basic responsibility and commitment of the company. Realization of security objective depends greatly on human elements. The alertness, prevention and responding effect only depend on the crew's security skill, knowledge, experience and attitude. The effective implementation of security assessment is favorable to make the continuously improvement of the ship security practice, and will constantly improve the security culture.

0.2 Risk-assessment-based decision-making

In order to reach the acceptable security risk level, the company and the ship must always identify potential maritime security threats the ship is likely to be encountered, and must systematically and scientifically analyze the possibility of security damage likely to be caused by the ship and its personnel, cargoes equipment, technical system and operation, and its seriousness of the consequence, and determining the process of the actions taken to mitigate the unacceptable risk, all of which are called "risk-assessment-based decision-making".

0.3 Risk and risk management

Risk can be shown through the probability and consequence of a given security tampering as the following equation:

$$R = PC \qquad (1)$$

where: R — risk value of a given security tampering;

P — probability of a given security tampering. The probability of security tampering can be further defined as the product of the threat (*T*) and vulnerability (*V*), i.e. $P = TV$ (2);

C — the sum likely to be resulted from a successful security incident. The consequence can be based on life, economy, symbolized value, environmental influence etc.

In accordance with the principle of risk management, it is generally considered that risk always exists and cannot be eliminated thoroughly. However, risk can be mitigated through management so as to reduce the extent of the consequence (*C*), to prevent the threat (*T*), or to mitigate the vulnerability (*V*). It is usually easier to mitigate vulnerability than to reduce the consequence or threat. The final objective of risk management is to reach a comparatively low risk level. The objective of maritime security is to endure that when threat level increases, the threat can be offset by means of the actions taken to reduce the consequence (*C*) or to reduce the vulnerability (*V*). For example, a ship at a port can takes actions to add security check when threatened with bomb. Another example is that the ship can require cease of cargo handling, boarding control of personnel from outside, or shifting the ship far from the easily attacked location when lack of ship security officer.

1 Objective and application

1.1 The ship security assessment procedures and principles provided in the Guidelines are applicable to the implementation related to ship security assessment in accordance with International Code for the Security of Ships and of Port Facilities, and are also applicable to any ships and water surface installations seeking good practice of security management.

1.2 The purpose of the Guidelines is to provide the company and personnel implementing ship security assessment with a set of reasonable, feasible and systematic security assessment method so as to instruct the company and/or the ship in their establishment, implementation and maintenance of the ship security system.

(1) developing implementation procedure of security assessment;
(2) preparation of information and personnel needed for implementing security assessment;
(3) requirements for identification of documents.

2 Definitions

(1) 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, or the ship from the risks of a security incident.

(2) 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.

(3) 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 officer.

(4) Security threat means the status of potential threat determined to the ship, persons or port facilities in accordance with the threat situation and possibility.

(5) Illegal act means a criminal act to the ship, offshore derrick, persons, cargoes and port facilities.

(6) Status of damaged security means the consequence caused by an illegal act to the ship, properties, facilities and persons.

(7) Security incident means any deliberate suspicious act threatening the security of the ship, including a mobile offshore drilling unit, its crew, passengers, store and cargo, or of port facilities.

(8) Security level means the qualification of the degree of risk that a security incident will be attempted or will occur.

- Security level 1 (normal) means the level at which ships and port facilities are normally operate;
- Security level 2 (heightened) means the level applying for as long as there is a heightened risk of a security incident; and
- Security level 3 (exceptional) means the level applying for the period of time when there is the probable or imminent risk of a security incident.

(9) Key operation means all the operating activities likely to cause serious consequence of illegal boarding, illegal entry into restricted areas, a threat to the safety of the ship and persons, illegal action due to any human fault or ignorance.

(10) Restricted area means the sensitive areas (including access to these areas) likely to cause serious threat to the ship, persons etc., by those with the purpose of illegal attack, including any areas where danger will happen to the ship, persons onboard the ship and operation if these areas are damaged or spied on.

(11) Access to the ship means the possible means for persons outside the ship to board either legally or illegally.

(12) 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.

(13) 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.

(14) Ship security assessment means identifying vulnerability likely to cause the physical structure of ship security tampering, protection system, procedure of persons and other areas, and putting forward the process of the actions taken to eliminate and mitigate the vulnerability.

(15) Ship security identification means process of identifying the existence of maritime security threat and determining its characteristics.

Note: characteristics may include action mode to security tampering, security event, method of avoiding security incident, attacking object, etc.

(16) Risk means a combination of possibility and consequence of a special dangerous condition.

(17) Risk assessment means the whole process of evaluating the risk and determining whether the risk is tolerable or not.

(18) Security means the status of exempting unacceptable hazardous risk.

(19) Tolerable risk means the risk reduced to the extent acceptable to the company in accordance with the objective and maritime security policy of ISPS Code.

(20) Economy-based safety policy and objective means the measurable effect of ship security management system related to the maritime safety and security risk control of the company.

(21) Restricted condition means trading navigation areas, port facilities, construction of the ship, cargoes, persons related to ship security, including the assumption of the characteristics of the crew and passengers.

(22) Physical security means the part of the security management, the purpose of which is to arrange physical obstruct to prevent the attempt of intruding the security defense.

3 References

- Amendment to International Convention for the Safety of Life at Sea, 1974 adopted by the Diplomatic Conference on Maritime Security in December 2002;
- Part A and Part B of International Code for the Security of Ships and of Port Facilities;
- USCG NVIC 10-02 (Ship Security Guidelines).

4 Responsibilities

4.1 Company responsibilities

(1) The Company is to designate one company security officer or more. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the company operates provided it is clearly identified for which ships this person is responsible. The designated company officer and the way of his round-the-clock contact are to be indicated in the ship security plan.

(2) A ship security officer is to be designated for each ship. The designated ship security officer is to be able to carry out his responsibilities as specified in the ISPS Code. The chief officer or a person senior to the chief officer is recommended to be a ship security officer.

(3) The Company is to ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfill their duties and responsibilities in accordance with Chapter XI-2 of SOLAS Convention and Part A of the ISPS Code. The management support of the Company may include finances, qualified personnel, sufficient training, information, technology and equipment provision.

4.2 Responsibilities of company security officer

The company security officer is to be responsible for ship security assessment of each ship of the company’s fleet, so as to be in compliance with the provisions in Chapter XI-2 of SOLAS Convention and Part A of the ISPS Code.
The responsibilities of the ship security officer related to ship security assessment is, but not limited to, the following:

(1) advising the level of threats likely to happen to the ship, using appropriate security assessments and other relevant information;

(2) ensuring that ship security assessments are carried out;

(3) ensuring the development of the ship security plan, the submission for approval, and thereafter the implementation and maintenance;

(4) ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

(5) enhancing security awareness and vigilance;

(6) ensuring adequate training for personnel responsible for the security of the ship;

(7) ensuring effective communication and cooperation between the ship security officer and the relevant port facility security officers;

(8) ensuring consistency between security requirements and safety requirements;

(9) ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

(10) ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

4.3 Responsibilities of ship security officer

The responsibilities of the ship security officer related to ship security assessment is but not limited to the following:

(1) undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

(2) maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;

(3) proposing modifications to the ship security plan;

(4) enhancing security awareness and vigilance on board;

(5) ensuring that adequate training has been provided to shipboard personnel, as appropriate;

(6) coordinating implementation of the ship security plan with the company security officer and the relevant port facilities security officer;

(7) ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

(8) assisting company security officer with site security survey during ship security assessment.

5 Methods of ship security assessment

5.1 General

5.1.1 For development of the ship security plan, initial and overall ship security assessment is to be carried out so as to evaluate the effectiveness of security measures and procedures for preventing illegal action, and to determine the vulnerabilities of the ship against illegal action.

5.1.2 The result of the ship security assessment is to be used to determine the security measures needed to deal with local security threat considered onboard the ship.

5.1.3 Security level will change due to the changing of ships and time. In order make full use of ship and shore resources, communication between security officers is very important.

5.1.4 Ship security assessment is to determine:

a. need to protect goal;
b. security measures having been implemented;
c. additional security measures and procedures required.

5.1.5 Ship security assessment is to be subjected to regular review and the ship security plan is to be renewed as necessary.

5.1.6 Security assessment of each ship is to include the following two stages:

(1) The first stage is initial evaluation, determining the security threat of the ship under imitating condition of service characteristics, analyzing the risk extent of potential security threat which the ship is capable of dealing with.

(2) The second stage is final evaluation, identifying vulnerabilities of the ship to prevent security incident, security tampering through site security survey to determine acceptable risks, and determining the risk control measures to mitigate vulnerabilities for unacceptable risks.

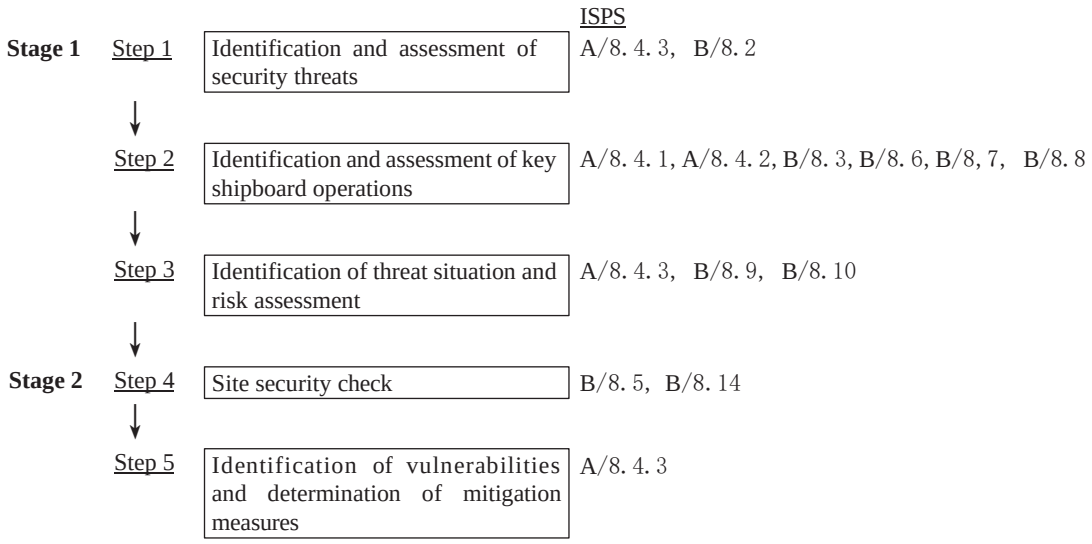
Note: The security assessment of a ship is to be carried out through two ways:

a. single ship — for single ship, security assessment is to be developed including required site security survey of the ship;

b. general-purpose ship — for general-purpose ship, security assessment is to be carried out covering the security risk assessment of the part or whole of the company's fleet, which is to provide "site security survey" for each ship. Ship security assessment reflects all the related "ship's characteristics".

5.1.7 The result of any ship security assessment is only applicable to specific service environment of the ship, including the structure condition of the ship, navigation areas, loaded cargoes. When the service environment of the ship changes substantially, the result of ship security assessment is to be reviewed, and the security is to be evaluated when necessary.

5.1.8 The steps and processes of ship security assessment



5.1.9 The following to be considered in ship security assessment

Security capability of the ship is to be evaluated under different security levels against security threat identified, including:

(1) physical security;
(2) structure integrity;
(3) personnel protection system;
(4) procedure policy;
(5) radio and radio communication system, including computer system and network; and
(6) restricted areas.

5.1.10 Personnel carrying out ship security assessment are to have risk evaluation knowledge and skill, and are to have expert assistant 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.

Note: Expert assistance can be realized by means of a person or a group of persons with the professional knowledge related.

5.2 Identification and evaluation of security threats

5.2.1 The purpose of security threat assessment is to evaluate the possibility of the ship when it is encountered the attack of illegal action under its restricted condition, and to order the various potential threats upon their threatening extents so as to further analyze the main security threats and put forward relevant control scheme.

5.2.2 Identification and evaluation of the threats of the ships' following factors are to be carried out by means of the analysis of the typical security events generally recognized by the maritime industry and other security information. The relativity between these factors is indicated in Table 1:

(1) the flag of the Administration the ship flies;
(2) the nature of the company which the ship belongs to;
(3) economy and dangerousness of the cargoes carried;
(4) the form of crew and passengers and their nationalities;
(5) the characteristics of the navigation areas / the arrival port.

Table 1

Characteristics of ship / Security incident	Relativity (great, medium, small, none)						
	Flag	Company	cargo	Crew	Passenger	Nav. area[2]	Port[3]
Terrorism incident[1]	Great	Great	Great	Great	Great	Great	Great
Robbery/hijack[4]	Small	Small	Great	Medium	Great	Great	Great
Pirate	Small	Medium	Great	Small	None	Great	None
Theft	Small	Small	Great	Small	None	Small	Great
Stealing into another country	Small	Small	Medium	Medium	Medium	Great	Great
Carriage of mass destruction weapons	Great	Great	Great	None	None	Great	Great
Carriage of criminals and equipment	Great	Great	Medium	Medium	Medium	Great	Great
Smuggle	Small	Great	Great	Great	Medium	Great	Great

Note: 1 Terrorism incidents include ship explosive, arson, malicious damage of public property, cargo damage, hijack, detaining persons as hostage etc.
2 Factor of navigation areas includes the navigation areas related to maritime security including terrorism-stricken areas, conflict areas, privacy areas, smuggling areas, indicative construction etc.
3 Port factor includes the port of a city with high international influence, close to densely populated area, with poor security condition, lack of protection, where major economic incident and political incident happens etc.
4 Hijack may also include terrorism incidents.

5.2.3 In accordance with the analysis in Table 1, when identifying ship security threats, the company security officer is to obtain the following information prior to ship security assessment for the effective assessment of security threats:

(1) ship information, including ship owner, company, cooperator of cargo trade, agent of crew, navigation areas and port;
(2) security status of the ship's navigation areas and arrival port;
(3) security guidance specified by the contracting government.

5.2.4 The information mentioned above may be obtained from:

(1) port state and flag Administration;
(2) recognized security organization;
(3) port Administration;
(4) agent;
(5) publication, such as IMO information;
(6) maritime organization and association;
(7) data from relevant website;
(8) past security incidents;
(9) master information;
(10) the company's management system.

5.2.5 Security threats of the navigation areas and ports the ship is servicing is to be paid special attention to in information collection, so that the main types of security threats and risk extents of navigation lines can be fully identified.

5.2.6 In accordance with the characteristics of ship business, potential security threat types of ships on navigation line or at port facilities of the intended navigation areas are to be determined, especially considering the factor of the cargoes carried. In combination of the risk extent in the navigation areas, the threat extent of ships in each navigation area and port is to be determined so as to provide basis of the appropriate security measures for the decision-making of the ships. The threat factors needed to be considered for various types of ships are provided in Table 2.

Table 2

Types of ships	Threat factor needed to be considered	Potential security incidents
Passenger ship, oil tanker	Factors of high value, flag, owner, anchoring country/ port, passengers of high incoming etc.	Terrorism incidents, robbery, piracy
Oil tanker,/ LPG/chemical tanker	Factors of sensitive cargo, potential environment influence, catastrophe result etc.	Terrorism incidents, robbery, piracy
Ro-ro passenger ship	Vulnerability to vehicle bomb, resulting in tampering, sinking, fire and personnel harm and loss	Terrorism incidents
Container vessel	Factors of hidden carriage of mass destructive weapons of specials cargoes, such as dangerous products, atomic material etc.	Piracy, robbery, carriage of mass destruction weapons, stowaway, smuggling
Bulk carrier		Piracy, robbery, carriage of mass destruction weapons
Other ships		Hijack, piracy, robbery

5.2.7 Working Table of evaluation and identification of ship security threats is give in 6 - Report of ship security assessment Form: SSAWF-03 of the Guidelines.

5.3 Identification and evaluation of key shipboard operations

5.3.1 The purpose of evaluation of key shipboard operations is to determine key shipboard operations, equipment, system, areas which are likely to be attacked and need special protection; to determine the extent of importance for evaluating ship security requirement; to provide information for determining the priority of security measures.

5.3.2 Key operation affecting ship security is shown in Table 3.

Table 3

Key shipboard operations	Factors of potential security threats	Security activity
Employed crew embarking	Disguised as crew, terrorism behave secretly and illegally	Crew enroll
Crew embarking & disembarking the ship	Utilized to be engaged in spy, overthrow and other illegal activities	Means of access control
Passengers embarking & disembarking and activities onboard	Criminals embarking as passengers, with weapons, bombing apparatus or dangerous goods, or engaged in illegal activities.	Ship/port cooperation Means of access control Control of restricted areas
Port facility personnel embarking & disembarking and activities onboard	Criminals embarking as passengers, with weapons, bombing apparatus or dangerous goods, or engaged in illegal activities. Stowaway, hiding criminals	
Outside businessmen embarking and activities onboard		
Outside unrelated personnel embarking and activities onboard		
Cargo handling	Carriage of contraband goods, explosive apparatus and dangerous goods, weapons including those of mass destruction	Cargo handling and surveillance
Ship navigation in narrow waters	Criminals easy to embark or directly attack the ship, including setting surface obstacle, due to the low speed of the ship and being close to shore	Ship navigation watch and lookout
Ship navigation with restricted visibility	Criminals easy to embark or directly attack the restricted visibility and low speed of the ship	
Ship mooring in port	Criminals embarking and disembarking at ease to behave illegally due to the factors of the small number of the crew, fatigue, responsibility, vigilance, and the tidal change	Mooring watch
Ship anchoring		Anchoring watch
Delivery of ship replenishment	Explosive apparatus, dangerous goods, drugs hidden in replenishment for ship	Replenishment supply ship
Repair of ship	Disguised as a repairman to damage the ship system stealthily	Access control Work surveillance

5.3.3 The following factors can be considered for the important evaluation of the key shipboard operations:

(1) performance and effect of ship safety operation;
(2) easy access to the personnel not allowed, weapons, explosive apparatus or dangerous goods;
(3) extent of environmental and economic influence;
(4) safety of ship operation;
(5) extent of recovery of ship's function.

5.3.4 The following information is to be obtained and recorded for evaluating key shipboard operations:

(1) Access to the ship includes the access to the ship and to the restricted areas onboard the ship for normal personnel and that for other personnel; the real function of the access.

(2) The restricted areas are the important locations for the operation, control and safety of the ship. They are to be fully identified through assessment. The restricted areas of the ship are to be indicated in the ship's general arrangement. They may include:

a. maneuvering console;
b. machinery control room;
c. radio/communication room;
d. type A machinery space and control station;
e. ventilating fan and its control room;
f. drinking water, pump, main pipe space;
g. security, surveillance equipment and system and their control space;
h. storage spaced of dangerous substance and cargoes, unaccompanied baggage;
i. cargo pumps and their control space;
j. crew and accommodation;
k. storage space for safety and emergency apparatus;
l. power control/equipment room;
m. light control room;
n. tiller-room;
o. cargo spaces;
p. storage areas of deck cargoes;
q. storage spaces of ship's spare parts and important repairing equipment;
r. spaces of emergency ship operation and spare equipment;
s. emergency exit, evacuation way and assembly station.

(3) Easily attacked areas and locations where appropriate control is needed. These spaces and locations include:

a. deck storage room;
b. cargo machinery storage room;
c. storage location for oxygen and acetylene cylinders.

Note: Different changes exist for access to the ship, restricted and unrestricted areas of different ships.

5.3.5 The commonly used key shipboard operations are listed in Form SSAWF-02 attached to Appendix of the Guidelines to provide a working table for identifying and evaluating key operations.

5.3.6 The sufficient identification and evacuation of key shipboard operations are to provide the basis of effectiveness and sufficiency of identifying and evaluating the security measures and procedures of the existing ships.

5.4 Identification of the security measures and procedures of the existing ships

5.4.1 The purpose of identifying the security measures and procedures of the existing ships is to determine ship security capacity for the security operation under three security levels of the ship, so as to identify the determination of the risk extent of the ship responding to its potential security threat and the determination vulnerability of unacceptable risk.

5.4.2 Security measures and procedures of the existing ships may include the following:

(1) check and control procedures;
(2) identity identifying system;
(3) monitoring and surveillance equipment;
(4) personnel identity documents;
(5) communication system;
(6) alarm system;
(7) lighting system;
(8) access control system.

5.4.3 The information of the security measures and procedures mentioned above is to be investigated, and the applying effectiveness under its regular and emergency condition is to be researched, so as to determine the adoption of the guidance principle with good security including the following:

(1) restricted areas;
(2) monitoring extent to crew, passengers, visitors, sellers, repairman, port facility personnel;
(3) areas, scope and frequencies of security patrol;
(4) access control system, including identification system;
(5) security communication system and procedures;
(6) locks, fences and lighting system;
(7) security surveillance equipment and system;
(8) emergency procedures for the other emergency status such as fire, bomb threat, hijack or seizure of the ship or persons onboard etc.

5.4.4 The security measures adopted for each identified key shipboard operations may be determined in the working table (FORM: SSAWF-02) attached to Appendix of the Guidelines, appropriate key words are to be identified through evaluation so as to identify the nature of the existing measures.

5.4.5 The limit and insufficiency of the security measures is to be evaluated for the identified ship operation, system, areas and persons.

5.5 Identification of threat scenarios and risk assessment

5.5.1 Identification of threat scenarios

(1) Threat scenarios are the potential security threat the ship encounters. It is the means of the concrete attack the ship may encounter. The threat scenarios are to be the combination of the security and the concrete objective of the ship.

(2) Two main types of threat scenarios of ships and the form of expression are provide in Table 4.

Table 4

Attack type	Security incident	Form	Means
Above waterline	Explosion	Suicidal attack Boarding stealthily (weapons and bomb) hidden in cargo or supplies Boarding without hindering	• Body bomb (worker, visitor boarding) • Vehicles (harbour) • Small plane (anchorage or in navigation)
	Deliberate damage		• Crew or port workers • Not formal access (ship side, anchor chain, cable) • With cargo or suppliers, e.g. stowaway
	Piracy		• Boarding from water (small craft) • Boarding from harbour (vehicle)
	Smuggling		
Below waterline	Deliberate damage	• Under water goal such as rudder, propeller etc., resulting in sinking of the ship or the ship unable to move. • Damage of hull	Diver
	Under water explosion		Mini submersible

(3) The typical ship security threat scenarios are provided in Table 5.

Table 5

Typical threat scenarios		Scope
1 Intrusion and/ or control of ship and …	1 Damage/destroy vessel with explosives	Intruder plants explosives
	2 Damage/destroy vessel through malicious acts	Intruder controls the ship and makes it grounded or runs it into another object; releasing the dangerous substance by opening the valves to damage the ship (e.g., setting fire making explosion on the ship)
	3 Create a pollution or toxic release incident without destroying target	Intruder opens valves/vents to release toxic substance; overrides interlocks resulting in damage/ destruction
	4 Take hostage/kill people	Goal of intruder is to kill people
	5 Disable critical vessel services (e.g., propulsion, steering and power)	Intruder creates damage to critical shipboard equipment so vessel is vulnerable to grounding
2 External attack by...	1 Moving explosives adjacent to vessel • from the waterside, • the shore side, • subsurface	Vehicle/train bomb Diver/swimmer lays explosives
	2 Ramming a stationary target • with a vessel and/or with a land based target	Intentional collision meant to damage-destroy the target
	3 Stand off attack – launching or firing weapon from a distance	Firing at the vessel with a missile or rifle
3 Using the vessel as a means of transferring…	1 Materials to be used as a weapon in/out of the country	
	2 Transporting persons into/out of the country	

(4) Uncertain factors exist during identifying ship security threat scenarios. It is unnecessary to be in details, only to consider the factors of the ship's characteristics such as crew, cargoes, trading areas, port etc. Brain-storming may be adopted.

(5) If the steps used for identifying and evaluating security threat in 5.2 are not pointed to the special threats of the ship, the standard list of the possible security threat scenarios as mentioned in Part B/8.9 of the ISPS Code. If the special security threat is encountered, the standard list may be specially detailed. The working table is provided in FORM: SSAWF-03 attached to Appendix of the Guidelines, including ship security threat scenarios as mentioned in Part B/8.9 of the ISPS Code.

(6) When evaluating possible security threat scenarios of the ship, the information of identification and evaluation in 5.2 to 5.4 is to be fully considered, including:

a. security threats;
b. key operation of ship security needs considering in priority;
c. existing security measures and procedures.

5.5.2 Risk assessment

(1) The purpose of risk assessment is to determine security threat risk level of the ship, and to identify and evaluate the factors affecting risk level, so that decision-making of security measures is to be concentrated on high risk level and affected risk level. At the same time, the relationship among shipboard activities, operation, areas, equipment, system, infrastructures and the consequence of the vulnerabilities easily attacked in security system and security tampering/incidents is to be identified so as to make security measures to mitigate risk.

(2) The risk level is to be determined to the security threat scenarios of each identified ship mentioned in 5.5.1 through the possibility of successful attack and the seriousness of possible consequence caused. The risk level shows the vulnerable extent of the ship security capacity responding to security threats.

(3) The consequence evaluation of the security threat scenarios is based on the consideration of three factors of casualties, economic loss and environment influence, and to be scored at different levels. If the consequence seriousness is catastrophe, major and medium, they can be scored as 3, 2 and 1 respectively.

(4) The possibility of successful attack of the security scenarios is based on the consideration the two factors of the accessibility and organizing security in ship security capacity. The possibility can be scored to be possible and impossible respectively.

(5) The working table in FORM SSAWF-03 attached to Appendix of the Guidelines may be used to evaluate the risk assessment of the ship security threat scenarios. The vulnerability score of the ship security level of each security scenario is to be determined. The vulnerability score of the unacceptable risk is to be determined to adopt mitigating measures.

Major vulnerabilities of each security threat scenario are to be determined for unacceptable risk. The shipboard operation, areas and activities needed to adopt security measures include:

a. access control;
b. restricted areas;
c. cargo handling;
d. delivery of ship supplies;
e. handling of the unaccompanied baggage;
f. security monitoring.

5.6 Site security survey

5.6.1 Site security survey is the part composed of the ship security assessment, the purpose of which is to determine that the ship security plan reflects the ship's characteristics.

5.6.2 The site security survey is to be carried out on the basis of completion of the information assessment mentioned in 5.2 to 5.3 and completion of the security threat risk assessment, and to make a site survey list in accordance with the information collected, so as to ensure the effectiveness and sufficiency of the site security survey.

5.6.3 During site security survey, the accuracy of the information collected in the initial stage is to be determined. The detailed security measures of the three security levels as specified in ISPS Code are finally to be determined.

5.6.4 The existing security measures, procedures and operation are to be inspected and evaluated during the security survey, including following emergency and regular operation status:

(1) responsibility and post of the persons onboard, added security task, influence to the ship security operation;

(2) existing security communication procedures and measures, the requisite measures to keep continuous communication when encountering security threats;

(3) procedures for evaluating security status, the procedures to keep security monitoring equipment and system continuously effective (including the procedures for identification of and responding to the security equipment or system deficiency or failure);

(4) the procedures and practice to protect sensitive information;

(5) maintenance of security equipment and system;

(6) control of dangerous goods;

(7) crew boarding;

(8) restricted areas;

(9) cargo handling and delivery of ship's store;

(10) handling of unaccompanied baggage;

(11) security monitoring methods;

(12) emergency measures including safety equipment, emergency evacuation routes, emergency plan.

5.6.5 Site security survey is to identify and evaluate the methods and procedures used for the control of access including:

(1) inspection, control and monitoring of persons and their effects;
(2) inspection, control and monitoring of cargoes, ship's supplies and baggage.

5.6.6 Each access is to be inspected including weather deck in order to evaluate that they are likely to be utilized by the person engaged in illegal actions, including entry into the access as a person with legal identity or an attempt to enter it without permission.

5.6.7 A Checklist of ship security inspection is provided in FORM SSAWF-04 attached to Appendix of the Guidelines. Shipboard operation procedures and specifications implemented onboard are to be inspected through talk with the personnel onboard the ship. Site physical inspection is also to be carried out to check each item on the Checklist of ship security inspection and then to evaluate and record what is detected.

5.7 Identification of vulnerabilities and mitigating measures

5.7.1 Vulnerabilities of the ship security measures are to be identified through site security inspections, and the improving measures are to be analyzed and determined.

5.7.2 The effectiveness of improving measures made for the ship security vulnerabilities is to be evaluated through vulnerability extent obtained from risk assessment mentioned in 5.5.2.

6 Report of ship security assessment

6.1 Development and approval of ship security assessment report

6.1.1 After completion of the ship security assessment, the company security officer is to organize personnel to prepare the assessment report which is to include:

(1) implementation summary of the ship security assessment;
(2) assessment of each vulnerability detected;
(3) corresponding measures to solve the vulnerabilities.

6.1.2 The content of the ship security assessment report may be referred to in the Form of ship security assessment report in Appendix of the Guidelines.

6.1.3 The ship security assessment report is to be reviewed and approved by the personnel organized by the company security officer. If the ship security assessment is not carried out by the company, the company security officer must review and approve the report.

6.1.4 The security assessment report is to be kept secret, any access to and disclosure of the report is not allowed without being authorized.

6.2 Periodical assessment and re-assessment

6.2.1 If the following changes of the ship take place, the company security officer is to organize personnel to carry out security assessment again, including site security survey:

(1) changing of the shipping lines of the company;

(2) changing of the ship's management and operation, such as major adjustment of the crew including numbers, sources, and changing of the ship's use;

(3) major changes of the ship structure, security equipment and system.

6.2.2 Periodical review is to be carried out to the ship security assessment under following conditions, and the corresponding amendment is to be made to the assessment report and the security plan where necessary.

(1) the interval of twelve months;
(2) the result of drills and exercises considered necessary;
(3) major security event happens, and where considered necessary.

Appendix Ship Security Assessment Report

Ship Security Assessment Report

1. Ship's particulars

Name of ship		Type of ship	
Flag of ship		Working language	
Port of registry		Nationalities of crew	
Registered number		General navigation areas	
Call letters		General port of destination	
IMO number		Class	
Gross tonnage		Class register number	

Date of ship security assessment		assessed by:
Date of site security survey		Implemented by:
Place of site security survey		

CSO Review and acceptance

Comments:			
Date of CSO approval		Signed by CSO	

2. Summary of ship security assessment methods

Stages	Steps		ISPS requirements	Working table
First	Step 1	Identification and evaluation of security threats	A/8.4.3, B/8.2	SSAWF-01
	↓			
	Step 2	Identification and evaluation of key shipboard operations	A/8.4.1, A/8.4.2, B/8.3, B8.6, B/8.7, B/8.8	SSAWF-02
	↓			
	Step 3	Identification of threat scenarios and risk assessment	A/8.4.3, B/8.9, B/8.10	SSAWF-03
	↓			
Second	Step 4	Site security inspection	A/8.5, B/8.14	SSAWF-04
	↓			
	Step 5	Identification of vulnerabilities and mitigating measures made	A/8.4.3	SSAWF-03

FORM SSAWF-01

Working Table for Identification of Ship Potential Security Threats

Security threat factors		Description	Likelihood			Comment
			U	P	L	
1	***Factors of ship company, flag of ship***					
1.1	Does it exist political (incl. religious, ideological, ethnical, nationalistic) motives related to flag of your ship?	Flag of ship：_____				
1.2	Does the visibility or the profile of your ship, company or brand represent a motive for unlawful acts?	Trade representative of the country ☐ political attitudes ☐ Weapons ☐ natural resources ☐				
2	***Factors of ship and the cargoes***					
2.1	Can your ship be used as a means to damage or endanger or escalate consequences and thus create fear in the society?	Type of ship：_____ explosion ☐ fire ☐ release of toxic gas ☐ nuclear radiation ☐ numerous fatalities of passengers ☐				
2.2	Are there any motives of your ship which will encounter illegal actions?	Carrying special goods such as weapons, nuclear materials etc. ☐ Carrying natural resources in dispute ☐ Carrying major engineering equipment ☐ Others：_____ ☐				
2.3	Is the trade your ship represents critical to society?	Oil transportation ☐ Critical materials for ind. production ☐ Others：_____ ☐				
2.4	Will an unlawful act against your ship or trade harm the state of the industry?	Reduced market due to reduced trust ☐				
2.5	Does your ship, cargo or passengers represent risk for hijacking?	Valuable ship ☐ Valuable cargo ☐ Valuable passengers ☐ Others _____ ☐				
3	***Crew factors***					
3.1	Is it likely that your crew can take part in or embrace terror related smuggling	Racial cause ☐ Others ☐				
3.2	Is it likely that your crew take part in or help others stow away					
4	***Navigation areas and port***					
4.1	Does your ship trade in an area with unstable political situation?	Elections ☐ Demonstrations ☐ civil war ☐ Riots ☐ others ☐				
4.2	Does your ship visit a port where international events take place?	Exhibitions ☐ Sports ☐ Political ☐ Others ☐				
4.3	Are there any indicative buildings or tourist attraction along the route?	Famous buildings ☐ Statues ☐ Bridges ☐ Others ☐				
4.4	Do unlawful acts take place frequently on the route of your ship?	Piracy ☐ Smuggling ☐ Stowaway ☐ Terrorism ☐				

Notes： 1 U—Unlikely P—Probably L—Likely

2 The analysis result of the ship and the company factors in 1 of the table may be used to evaluate the general possibility when the ship encounters the attack of the security threats.

3 The analysis result of the other threat factors in the Table may be used to determine the possibility of the type of potential security threat scenarios.

4 The threat factors can be analyzed in accordance with the information announced by the related international organizations and state Administration and the experience of the company.

5 Brain-storming may be used in threat assessment.

Working Table for Key Shipboard Operations and Security Measure Assessment

FORM: SSAWF-02

Key operations with related systems, areas and personnel		Locations (can be identified in general layout)	Criticality		Security measures in place		Existing measures, procedures, operations, vulnerabilities and their limits
			L	H	Y	N	
1	***Access control — personnel, passengers, visitors and their baggage***						
1.1	Access ladders						
1.2	Access gangways						
1.3	Access ramps						
1.4	Access doors,side scuttles,windows and ports						
1.5	Mooring ropes						
1.6	Anchor chains						
1.7	Cranes and hoisting gear						
1.8	Ships side (freeboard)						
1.9	Baggage brought onboard						
1.10	Unaccompanied baggage found onboard						
	(any other access)						
2	***Restricted areas on the ship***						
2.1	Navigation bridge						
2.2	Machinery spaces						
2.3	Power supplies						
2.4	Steering rooms						
2.5	Control rooms (fire protection)						
2.6	Radio/communication room						
2.7	Crew and accommodation						
2.8	Cargo spaces						
2.9	Store rooms of spare parts and equipment						
2.10	Ventilation and air conditioning system						
2.11	Living spaces of the crew						
2.12	Kitchen/canteen						
2.13	Hull and ballast tanks						
2.14	Rudder and propeller						
2.15	Storage of dangerous substance						
2.16	Navigation means						
	Add issues you find relevant						
3	***Cargo handling***						

Key operations with related systems, areas and personnel		**Locations (can be identified in general layout)**	**Criticality**		**Security measures in place**		**Existing measures, procedures, operations, vulnerabilities and their limits**
			L	H	Y	N	
3.1	Cargo access points (hatches, ports, pipings)						
3.2	Cargo storage spaces						
3.3	Cargo handling equipment						
4	***Ship stores handling — stores, spare parts, food, daily necessities***						
4.1	Access points for delivery to ship						
4.2	Storage spaces						
4.3	Access points to storage spaces (doors and windows etc.)						
5	***Ship security monitoring***						
5.1	Lighting						
5.2	Watch-out						
5.3	Security guards and deck watches, including patrols						
5.4	Automatic intrusion detection advice						
5.5	CCTV surveillance monitoring						
6	***Safety operations***						
6.1	Life appliances (boats, rafts, jackets and belts						
6.2	Alarms, signals and marking						
6.3	Emergency evacuation routes						
6.4	Fire fighting system						

Threat Scenarios and Risk Assessment FORM SSAWF-03

Ship: _____ **Flag:** _____ **Route:** _____ **Assessment date:** _____ **CSO** _____ **SSO** _____

Identification of potential threats			**Threat security assessment**					*Measures to mitigate vulnerabilities*				*Assessment of effectiveness of the measures taken for mitigation*
Threat scenarios	**relevant**		**Seriousness of consequence**			**likelihood**		**Vulnerability score**			**Mitigation measures**	
	Y	**N**	**moderate 1**	**high 2**	**extreme 3**	**Likely 1**	**Unlikely 2**					
1. Dahip (bombing, arson, sabotage, vandalism) mage to, or destruction of, the s												
1.1 Hide explosives onboard, initiate with timer/remote												
1.2 Bring explosives onboard, suicidal/high risk action												
1.3 Place explosives in cargo, initiate with timer/remote												
1.4 Attach explosives to hull, initiate with timer/remote												
1.5 Explode ship by external craft, torpedo, mine, etc.												
1.6 Force oil/gas leakage: engine room/cargo tanks												
1.7 Set ship on fire												
1.8 Open bow port, cargo hatch (to sink or capsize)												
1.9 Drain holes, to sink or capsize												
1.10 Cut pipes (water intake) to change trim												
1.11 Activate pumps to change trim												
2. Hijacking or seizure of the ship or of persons onboard												
2.1 Crew takes control over ship												
2.2 Stowaways/boarden person take control over ship, leading to environmental catastrophe												
2.3 hijacking through (bomb) threat												
2.4 Hijacking of crew												
2.5 Unlawful detention of ship/crew by port authority or state												
3. Tampering with cargo, essential ship equipment or system or ship's stores												
3.1 Block critical systems like propulsion steering etc												

Identification of potential threats			Threat security assessment					*Measures to mitigate vulnerabilities*				*Assessment of effectiveness of the measures taken for mitigation*
Threat scenarios	**relevant**		**Seriousness of consequence**			**likelihood**		**Vulnerability score**			**Mitigation measures**	
	Y	**N**	**moderate 1**	**high 2**	**extreme 3**	**Likely 1**	**Unlikely 2**					
3.2 Contaminate bunker												
3.3 Damage ship system, navigation, loading												
3.4 False navigation data/guidance (radar, VTS, pilot, chart)												
3.5 Contaminate drinking water or food												
3.6 Release gas onboard												
3.7 Contaminate substance												
3.8 Destroy lifesaving equipment												
3.9 Destroy ship interiors												
4. Unauthorised access or use including presence of stowaways												
4.1 Stowaways sneaking onboard/hiking in cargo												
4.2 Boarding ship at port or during voyage as “passenger” or “crew”												
4.3 Boarding ship at port during voyage as “pilot”, “supplier”, “surveyor”, fake castaway												
4.4 Unauthorized boarding ship at pilot entrance or STS operations												
4.5 Unauthorized boarding ship at voyage via vessel / craft / helicopter												
4.6 Unauthorized boarding ship at voyage via shipwrecked												
(Unauthorized use, see item 5)												
5. Smuggling weapons or equipment, including weapons of mass destruction												
5.1 Hide weapons in cargo												
5.2 Hide weapons in crew’s luggage												
5.3 Hide weapons in ship supplies												
6. Used the ship to carry perpetrators and their personal equipment												
6.1 Stowaways sneaking onboard / hiding in cargo												

Identification of potential threats			**Threat security assessment**					*Measures to mitigate vulnerabilities*				*Assessment of effectiveness of the measures taken for mitigation*
Threat scenarios	**relevant**		**Seriousness of consequence**			**likelihood**		**Vulnerability score**			**Mitigation measures**	
	Y	**N**	**moderate 1**	**high 2**	**extreme 3**	**Likely 1**	**Unlikely 2**					
6.2 Boarding ship at port or during voyage as "port facility personnel" or "crew"												
6.3 Boarding ship at port or during voyage as fake "pilot", "supplier", or similar												
7. Use of the ship itself as a weapon or as a means to cause damage or destruction												
7.1 Crew take control over the ship												
7.2 Stowaways/boarden person take control over the ship												
7.3 Blocking critical systems like propulsion, steering etc in a critical position (near terminal etc)												
7.4 Given a hijacked situation (item 4): Take control over the ship and hit another ship												
7.5 Given a hijacked situation (item 4): Take control over the ship and hit a land-based construction / terminal / chemical plant or similar												
7.6 Given a hijacked situation (item 4): Take control over the ship and hit an offshore installation												
7.7 Given a hijacked situation (item 4): Take control over the ship and hit a rock / provoke grounding												

Notes: 1. Vulnerability score = likely consequence + likelihood.

2. Mitigation measures are to be taken when the vulnerability score is more than 4.

A: access control; B: determination of the restricted areas and control; C: cargo handling control;

D: delivery of ship stores and control; E: handling of unaccompanied baggage; F: security monitoring.

3. Assessment of the effectiveness of measures for mitigation. New vulnerability score is to be determined in accordance with 1 above, to evaluate the effectiveness.

Checklist of Ship Security Inspection FORM：SSAWF-04

Ship：_____ Type：_____ Route：_____

Inspection date：_____ Inspected by：_____

Part 1 — Security Management

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
1. Company security management and policy					
A	Are the master, ship security officer (SSO), and crew familiar with the company's security objective and policy?				
	Are adequate resources, including shore based support, provided for the ship to meet the goals of the company security policy?				
2. Company security officer (CSO)					
	Are the ship security officer and master knowledgeable about how to contact the CSO?				
A	Does the CSO arrange for internal audits of security activities?				
A	Is the CSO promptly addressing deficiencies and non-conformities?				
A	Does the CSO provide adequate training for personnel responsible for the security of the ship?				
A	Is the CSO ensuring effective communication and co-ordination between the ship security officer and the relevant port facility security officer?				
A	Is there evidence that the CSO is working to enhance the security awareness and vigilance onboard?				
3. Ship security officer (SSO)					
A	Is the SSO qualified as a security specialist (e.g., through special training and/or education)				
A	Is the SSO aware of his responsibilities and duties, including his reporting lines?				
A	Is there evidence that the SSO is undertaking regular security inspections of the ship				
A	Is there evidence that the SSO is reporting all security deficiencies, non-conformities, and security incidents?				
A	Is there evidence that the corrective actions are implemented?				
4. Master					
A	Is it established in the SSP that the master has the overall responsibility for the ship's safety and security?				
	Is there evidence that the master is aware of his full responsibilities, e.g.: • Ship security plan, • Ship security implementation and maintenance • Master's responsibility to request company assistance if necessary				
	Master has available onboard updated documented information on who appoints the crew, who decided and decides the employment of the crew, and who signed and signs the charter party.				

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
	Is there evidence that master (and the SSO) is providing ongoing motivation of crew with respect to ship security, as described in the SSP?				
5. Ship's personnel					
	Is the crew familiar with the company security policy and the related procedures, as described in the SSP?				
	Is there evidence about the crew's awareness in security related issues (e.g., access control of people, cargo control, restricted areas onboard, responsibilities in case of security threats, etc)?				
	Does the crew know who is appointed to the different security duties?				
	Does the crew know how to respond to an attack or threat situation? (e.g., activate alert system?)				
6. Training and qualifications					
A	Are needs for security training identified and onboard training programs made for new and existing crew?				
A	Have the crew received adequate training in security matters, as described in the SSP?				
A	Is the security training properly recorded?				
7. Ship security plan					
A	Is periodical review of the ship security plan carried out as specified?				
A	Are all changes to the security plan in compliance with the requirements, and approved by the Administration?				
A	Is the security plan properly protected from unauthorized access or disclosure?				
	Is the ship protecting security sensitive information, available either electrically or on paper?				
8. Ship security surveys, security audits					
A	Are (internal) security audit performed onboard in accordance with the procedures in the SSP?				
A	Are the internal audits carried out by personnel independent of the activities being audited?				
A	Is security inspection carried out periodically				
9. Security records					
A	Are records of training, drills and exercises kept onboard?				
A	Are records of reports of security incidents kept onboard?				
A	Are records of breaches of security kept onboard?				
A	Are records of changes in security level kept onboard?				
A	Are maintenance, calibration and testing of security measures and related equipment kept onboard?				
A	Are records of communications relating to the ship kept onboard?				
A	Are records of internal audits and reviews of security activities kept onboard?				
	Are records with memos from onboard security meetings kept onboard?				
10. Ship/shore interface					

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
	Is the SSO communicating and co-ordinating security issues with the PFSO?				
	Is port specific information (e.g. threats and their protective measures) readily available?				
	Are PFSO/CSO/contracting security Administration informed of fact that the security level of the ship is higher than that of the port in accordance with the relevant procedures				
	Is a Declaration of Security issued onboard? Are the reason and content of the issuance in compliance with the requirements?				

Part 2 — Onboard security measures

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
1. Access to the ship					
	Are access ladders identified and monitored?				
	Are access ramps identified and monitored?				
	Are access gangways identified and monitored?				
	Are access doors, side scuttles, windows and ports identified and monitored?				
	Are mooring ropes and anchor chains identified and monitored?				
	Are cranes and hoisting gear identified and monitored?				
	Are other access points identified in the SSA?				
	Are identity documents of all persons seeking to board the ship checked?				
	Are there procedures and records available for how to check this?				
	Are the reasons for the people boarding the ship confirmed by checking joining instruction, passenger tickets, boarding passes, work orders etc?				
	Are the personnel effects of passengers controlled?				
	Is the embarkation of crew controlled? Is the bulletin board put up at boarding entrance?				
	Are the personal effects of crew controlled?				
	Are there procedures on how to check any other people accessing the ship (e.g. visitors, vendors, repair technicians, port facility personnel etc)?				
	Are the designated secure areas established (in coordination with the port facility) where inspections and searching of people, baggage (including carry on items), personal effects, vehicles and their contents can take place?				
	Are vehicles destined to be loaded onboard car carriers, ro-ro and other passenger ships searched prior to loading in accordance with the frequency required in the SSP?				
	Are checked persons and their effects segregated from unchecked persons and their effects?				
	Is the embarking passengers segregated from the disembarking passengers?				

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
	Are unattended spaces adjoining areas to which passengers and visitors have access secured, by locking or other means?				
	Are security briefings provided to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance?				
	Are there procedures for how to raise alarm and to react if unauthorised boarding is detected?				
	Are there procedures for checking persons boarding the ship as a result of a rendering assistance at sea?				
	Are locations and functions of each actual or potential access point to the ship identified?				
	Are evacuation routes and assembly stations defined and maintained?				
2. Restricted areas					
A	Are restricted areas defined, and where relevant, clearly marked?				
A	Is the ship's personnel (master, SSO, crew) able to identify the restricted areas onboard?				
	Is surveillance equipment (e.g. CCTV) used to monitor the restricted areas?				
	Are guards or patrols used to monitor the restricted areas?				
	Are automatic intrusion detection devices used to alert the ship's personnel of unauthorised access?				
	Are there measures to prevent unauthorised persons to access the navigation bridge?				
	Are there measures onboard to prevent unauthorised persons to access the machinery spaces (Category A)?				
	Are there measures onboard to prevent unauthorised persons to access the control stations (defined in ISPS Code, Chapter II-2)?)?				
	Are there measures onboard to prevent unauthorised persons to access the spaces containing security and surveillance equipment and systems and their controls and lighting system controls?				
	Are there measures onboard to prevent unauthorised persons to access ventilation and air-conditioning systems and other similar spaces?				
	Are there measures onboard to prevent unauthorised persons to access spaces with access to portable water tanks, pumps, or manifolds?				
	Are there measures onboard to prevent unauthorised persons to access spaces containing dangerous goods or hazardous substances?				
	Are there measures onboard to prevent unauthorised persons to access spaces containing cargo pumps and their controls?				
	Are there measures onboard to prevent unauthorised persons to access cargo spaces and spaces containing ship's stores?				
	Are there measures onboard to prevent unauthorised persons to crew accommodation?				
	Are there measures onboard to prevent unauthorised persons to access any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship?				
	Are restricted areas searched as part of the search of the ship?				

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
	Is the management of the keys onboard in compliance with the specification?				
	Are the locks and paper strict seals in good conditions?				
3. Handling of cargo					
	Are there routines in place for checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations?				
	Is there evidence, through records, that the procedures (cargo control) are followed?				
	Is the handling of cargo supervised by the ship personnel (SSO)?				
	Is there procedures for handling of dangerous goods or hazardous substances?				
	Is an updated inventory kept on any dangerous goods or hazardous materials carried onboard?				
	Are any checks carried out to ensure that cargo being loaded matches the cargo documentation?				
	Are there procedures ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP?				
	Is checking of seals or other methods used to prevent tampering?				
	Is the cargo checked visually or by examinations?				
	Is scanning or detection equipment, mechanical devices or dogs being used for checking?				
4. Ship’s stores					
	Are there procedures in place for supervision of the delivery of ship’s stores (to prevent acceptance without inspection)?				
	Are there procedures for handling of ship’s stores to prevent acceptance unless ordered?				
	Is there evidence, through records, that the procedures (ship’s store control) are followed?				
	Is the ship’s stores and package integrity being checked?				
	Are stores checked if matching the order prior to being loaded on board?				
	Is immediate secure stowage of ship’s stores ensured?				
5. Unaccompanied baggage					
	Are there procedures in place for how to handle and where to store unaccompanied baggage?				
	Is there evidence the procedures are followed?				
	Is any unaccompanied baggage been appropriately screened (100%) and searched (by port or ship), before it is loaded onboard the ship?				
	Are there procedures and measures in place for close cooperation with the port facility to ensure that unaccompanied baggage is handled securely after screening				
	Is the ship refusing to accept unaccompanied baggage on board?				
6. Monitoring the security of the ship					

Security Code ref.	Security measures	Y	N	Findings	Corresponding measures
A	Are there procedures for inspection, testing, calibration and maintenance of any security equipment onboard?				
	Are the restricted areas being monitored? (see also item 2)				
	Are the deck areas being monitored?				
	Are the surrounding areas being monitored?				
	Is the security communication equipment readily available?				
	Is the security information readily available onboard?				
	Is security equipment installed onboard maintained, working properly, and readily available?				
	Are the ship's deck and access points illuminated at all times while carrying out ship/port interface activities or at a port facility or anchorage?				
	Is the ship using the maximum lighting available while underway, consistent with safe navigation? (Having regard to the provisions of the 1972 COLREGS)				
	Is the lighting sufficient to ensure the ship's personnel to be able to detect activities beyond the ship, on both the shore side and the water side?				
	Is the lighting coverage including the area on and around the ship?				
	Is the lighting coverage facilitating personnel identification at access points?				
	Is the lighting coverage provided through coordination with the port facility?				
7. Security levels 2, 3					
	Has the security level been raised onboard?				
	Is the ship responding the change of the security levels in accordance with the requirements of the plan?				
	Is the responding security measures taken in accordance with the requirements of the plan?				
Others					
A	Is the security alert system working normally? (Does the alert system onboard activate when information is sent ashore?)				
A	Are there at least two points onboard at which the alert system can activate (one in navigation bridge and at least another one at other location)?				
A	Will the security alert system turned on unconsciously				
A	Are there procedures for the use of the security alert system onboard?				
A	Is the place where alert system can activate determined? (It must be recorded in the restricted / confidential document)				
	Can the AIS be normally operated at any time?				