

GUIDANCE NOTES  
GD018-2025



**INTERNATIONAL SHIP CLASSIFICATION**

**GUIDELINES FOR CERTIFICATION OF  
SHIP SECURITY SYSTEM  
(2025)**

**Effective from January 1, 2026**

## CONTENTS

### **Chapter 1 GENERAL**

### **Chapter 2 CERTIFICATION OF SHIP SECURITY SYSTEM**

Section 1 Certification of Security System

Section 2 Certificates

### **Chapter 3 APPROVAL OF SHIP SECURITY PLAN**

Section 1 General Requirements

Section 2 Documents to be Submitted

Section 3 Ship Security Plan

Section 4 Review of Documents

Section 5 Approval for Amendments to the Approved Ship Security Plan

### **Chapter 4 AUDIT OF SHIP SECURITY SYSTEM**

Section 1 General Requirements

Section 2 Initial Verification

Section 3 Periodical Verification

Section 4 Additional Verification

Section 5 Interim Verification

Appendix 1 ISPS Code Certification Scenarios - Minimum Requirements

Appendix 2 Form of ISSC

Appendix 3 Form of Interim ISSC

## Chapter 1 GENERAL

### 1.1. Application

1.1.1 International Ship Classification (hereinafter referred to as “the Society”) provides the service for certification of ship security system in accordance with the Guidelines for Certification of Ship Security System (hereinafter referred to as “the Guidelines”).

1.1.2 The Guidelines is applicable to the security system of the following types of ships engaged on international voyages:

- (1) passenger ships, including high speed passenger craft;
- (2) cargo ships, including high speed craft, of 500 gross tonnage and upward; and
- (3) mobile offshore drilling units.

1.1.3 The Society carries out the certification of ship security system based on an application submitted by the Company.

1.1.4 If the Society has been involved in either the conduct of the SSA or the development of the SSP or any amendments for a specific ship, the Society shall not, due to potential conflict of interest, approve the SSP or conduct verifications for the certification of the ship.

### 1.2. Equivalent

The Society considers that a ship security system is in compliance with the requirements of the rule, provided such ship security system is at least as effective as those prescribed in the rule.

### 1.3. Definitions and abbreviations

For the purpose of the Guidelines, unless otherwise specified, the following definitions apply in the Guidelines.

1.3.1. SOLAS means the International Convention for the Safety of Life at Sea, 1974, as amended.

1.3.2. ISPS Code means the International Code for Security of Ships and of Port Facilities adopted on 12 December, 2002 by Resolution 2 of Conference of Contracting Governments to SOLAS.

1.3.3. “Verification Criteria” means ship security requirements as deemed necessary by the Society as follows:

- (1) SOLAS reg. XI-2 / 4, 5, 6, 7 and 8;
- (2) SOLAS reg. XI-1 / 3, 5 and SOLAS reg. V / 19;
- (3) sections A/1.3, 5 to 13 of ISPS Code;
- (4) sections B/8 to 13 of ISPS Code;
- (5) the requirements of MSC/Circ.1074 measures to enhance maritime security interim guidelines for the authorization of recognized security organizations acting on behalf of the administration and/or designated authority of a contracting government Appendix 1, paragraphs 3 to 5.
- (6) special requirements of flag Administration (if any);
- (7) approved ship security plan.

1.3.4 “Ship Security System” means the system in place onboard the ship which implements the procedures, documentation and associated records which are examined to verify

- compliance with the requirement of the ISPS Code.
- 1.3.5 “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.
- 1.3.6 “Audit” means a process of systematic and independent verification by obtaining objective evidence to determine whether the ship security related activities comply with the ISPS-Code and the planned arrangements of the SSP and whether these arrangements are implemented effectively to achieve the objectives of the ISPS-Code.
- 1.3.7 “Security equipment” means the equipment used in the implementation of security measures specified in SSP.
- (1) Security equipment is one or more installations or measures installed, fitted and provided at one or more positions on a ship, used for prevent, monitor, detect and observe any potential security threat. Broadly speaking, security equipment includes equipment, apparatus, technical system, identification, closing appliance of a structure, etc.
  - (2) Some equipment has double functions, e.g. deck lighting is used both for the ship's normal operation and security functions.
- 1.3.8 “Ship's stores” mean:
- (1) materials that are on board a ship for the upkeep, maintenance, safety, operation or navigation of the ship;
  - (2) materials for the safety or comfort of the ship's passengers or crew, including any provisions for the passengers or crew.
- 1.3.9 “Sensitive information” means the information that can assist others (in the event that they get the information) with their plot to and attack on the ship security system. Sensitive information may include:
- (1) the information related to the security plan, arrangement
  - (2) vulnerability assessment report/information
  - (3) technical specifications and location of the security equipment
  - (4) the information of limitation of the security equipment
  - (5) sensitive e-mail, etc.
- 1.3.10 “Drill” means a training event that involves at least one component of the ship security plan and is used to maintain a high level of security readiness.
- 1.3.11 “Exercise” means a comprehensive training event that involves several functional elements of the ship or port facility security plan, and in which communication, coordination, resources available and response are tested.
- 1.3.12 “Verification” is confirmation through the evaluation of objective evidence that specified requirements have been fulfilled. The objective evidence may be obtained through observing, measuring, testing and other methods.
- 1.3.13 “Findings” mean the conclusions obtained from the appraisal of evidence collected during verification against verification criteria (1.3.3). Findings will show whether the verification criteria are complied with and will give opportunity for correction.
- 1.3.14 “Failure” means the non-fulfilment of a specified requirement that does not compromise the ship's ability to operate at security levels 1, 2 and 3. It may also be referred to as a Non-conformity.

- 1.3.15 “Major Failure” means the non-fulfilment of a specified requirement that compromises the ship’s ability to operate at security levels 1, 2 or 3. It may also be referred to as a Major Non-conformity.
- 1.3.16 “Observation” means a statement of fact made during an audit and substantiated by objective evidence. It may also be a statement made by the auditor referring to the SSP which, if not corrected, may lead to a Failure in the future.
- 1.3.17 “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.
- 1.3.18 “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.
- 1.3.19 “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 ship owner and who on assuming such responsibility has agreed to take over all the duties and responsibility imposed by the ISPS code.
- 1.3.20 “Certificate” means the International Ship Security Certificate (ISSC) or the Interim International Ship Security Certificate (Interim ISSC) issued in accordance with the requirements of ISPS Code.
- 1.3.21 “Periodical verification” means renewal verification or intermediate verification as specified in Section 3, Chapter 4.
- 1.3.22 “Anniversary date” means the day and the month of each year which will correspond to the expiry date of the relevant certificate or document.
- 1.3.23 “Document of compliance (DOC)” means the document referred to in SOLAS Reg. IX/4.
- 1.3.24 “Ship Security Alert System (SSAS)” means a system installed on board, either interfaced with another radio installation or self-contained (abbreviated to SSAS-SC), that complies with the functional requirements of SOLAS Chapter XI-2/6.2 to 6.4 and the performance criterion of IMO MSC.147(77).
- 1.3.25 “Automatic Identification System (AIS)” means equipment as required in SOLAS Reg.V/19.
- 1.3.26 “Continuous Synopsis Record (CSR)” means the record as required in SOLAS Reg.XI-1/5.
- 1.3.27 “Auditor” means a person trained, qualified and authorized by the society in accordance with PR10 to carry out SSP approval and audits on board.
- 1.3.28 “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.
- 1.3.29 Unless otherwise stated, terms not otherwise defined in the rule shall have the same meaning as the meaning attributed to those in SOLAS, ISM code and ISPS code.
- 1.4. Certification application and fees
- 1.4.1. A Company requesting certification of the ship security system and maintenance of validity of certificates of its certified ships is to submit a written application to the Society or its

local branches or the locations designated by it. If necessary, an agreement for certification service is to be signed with the Company.

1.4.2. Applicants are to pay certification fees, traffic fees and other related expenses in accordance with the Provisions of Survey Fees of the Society or agreements on certification service.

1.5. Responsibilities and limitation of liability

1.5.1. The society will sufficiently ensure the integrity and effectiveness of ship's ISPS certification, and when authorized to act on behalf of the flag Administrations, accept supervision of the Administrations

1.5.2. A certificate issued by the society is only a statement by the society that at the time of audit the ship had established and implemented a ship security system in accordance with the requirements in the Guidelines. It is possible that unauthorized change(s) made by the Company and/or the ship in the ship security system or their failure in effective implementation of the system due to subjective reasons thereafter will lead to noncompliance with the certificate issued. Compliance with all applicable requirements of the ISPS Code and the Guidelines remains the responsibility of the Company and/or the ship.

1.5.3. The maintenance of the certificate is conditional upon the ship's continued compliance with the requirements of the Guidelines. The society reserves the right to withhold, cancel the certificate or determine noncompliance with the certificate when the Company or the ship refuses the Auditor(s) of the Society access to the ship for verification, or fails to pay fees due on account of certification and other services, or there is evidence for failure of the Company or the ship in fulfilling their duties and responsibilities as specified in SOLAS.

1.6. Complaints and appeal

1.6.1. When the Company and/or a ship has any complaint against the verification of ship security system performed by the Auditor(s) of the Society, the Company and/or ship may appeal in writing to the location where the Auditor(s) serve. Where the opinion expressed by the location is still not considered satisfactory by the interested party, the latter may appeal in writing to the Headquarters of the Society giving detailed reasons for its request. The Headquarters will make the conclusion accordingly.

1.6.2. When the Company and/or a ship has any complaint against the conclusion drawn by a verification unit of the Society, the Company and/or ship may appeal in writing to the Headquarters of the Society giving detailed reasons for its request. The Headquarters will make the conclusion accordingly.

1.7. Availability of information ,confidentiality

1.7.1. Sufficient and correct information necessary for certification of ship security system is to be made available to the Society by the parties concerned.

1.7.2. The Society will not disclose any sensitive and proprietary information to which it has access during certification of ship security system to individuals and organizations not specified in the contract, including those staff members of the Society not concerned in the service, except as required by laws and regulations.

## **Chapter 2 CERTIFICATION OF SHIP SECURITY SYSTEM**

### **Section 1 Certification of Security System**

- 2.1.1 Certification of ship security system
  - 2.1.1.1 The Society will carry out the verification of the ship security system, to which paragraph 1.1 of the Guidelines applies, in accordance with Chapter 4 of the Guidelines, and will issue a relevant International Ship Security Certificate to the ship whose ship security system complies with the verification criteria (1.3.3) in accordance with the authorization by the flag Administration.
  - 2.1.1.2 The Society's certification service includes the approval of ship security plan and verification of ship security system. If the security plan of the ship requesting the verification has already been approved by the Administration or by the security organization recognized by the Administration, the Society may carry out the verification of ship security system involved in the ship security plan, and issue a relevant International Ship Security Certificate to the ship upon satisfactory completion of the verification.:
- 2.1.2 Maintenance of certification
  - 2.1.2.1 Periodic verification and additional verification, if required, are to be carried out for ship having obtained ISPS certification in accordance with the requirements of section 4, chapter 4 of the rule.
  - 2.1.2.2 Any change made to the ship security plan is to be submitted in a timely manner to the Society for approval. The Company shall not implement the changed ship security plan without the approval by the Society.
- 2.1.3 Information notification
  - 2.1.3.1 The Company and the ship obtaining ship's ISPS certification from the society are to immediately advise the society with security incidents of the ship and PSC detentions or expelled from a port due to failures of ship security, etc., within the validity of the certificate.

### **Section 2 Certificates**

- 2.2.1 Type and issuance of certificates
  - 2.2.1.1 Authorized by the flag State government, the Society is to issue certificates to the ships which have passed ISPS verification.
  - 2.2.1.2 The Society is to issue an interim ISSC at the interim verification as specified in Section 5, Chapter 4 of the Guidelines.
  - 2.2.1.3 The Society is to issue an ISSC at initial verification, renewal verification or at intermediate or additional verification involving change or re-issuance of certificates.
  - 2.2.1.4 In the event that the full-term ISSC is to be issued by the flag Administration, the Company shall apply for the full-term ISSC to the flag Administration by presenting the short-term ISSC issued by the society or the previous ISSC with endorsement to extend the

validity of the certificate and related verification report.

## 2.2.2 Validity of certificate

### 2.2.2.1 The validity of ISSC is to be in compliance with the following:

- (1) The certificates are to be valid for a period not exceeding five years from the date of completion of initial verification, subject to intermediate verification prescribed in the Guidelines during this period.
- (2) When renewal verification is completed within three (3) months before the expiry date of the existing certificate, the new certificate is to be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.
- (3) When renewal verification is completed after the expiry date of the existing certificate, the new certificate is to be valid from the date of completion of the renewal verification for a period not exceeding five years since the expiry date of the existing certificate.
- (4) When the renewal verification is completed more than three (3) months before the expiry date of the existing certificate, the new certificate is to be valid from the date of completion of the renewal verification for a period not exceeding five years.
- (5) If the renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the existing certificate may be endorsed and such a certificate is to be accepted as valid for a further period not exceeding five (5) months from the expiry date.
- (6) At the request of the Company, the validity of an ISSC can be harmonized with the validity of SMC, subject to the validity of ISSC certificate not exceeding five years as specified in A/19.3 of ISPS Code.

2.2.2.2 The validity of the interim ISSC shall valid for not more than six (6) months from the completion date of the verification as specified in 4.4.2 of the Guidelines.

2.2.2.3 If an intermediate verification is completed before the period specified in Section 3, Chapter 4 of the Guidelines, the expiry date shown on the certificate is to be amended by endorsement to a date which is to be not more than three years later than the date on which the intermediate verification was completed, unless one or more additional verifications are to be carried out.

## 2.2.3 Extension of certificate validity

2.2.3.1 If a ship at the time when the certificate expires is not in a port in which it is to be verified, the Society may extend the period of validity of the ISSC certificate if permitted by the Administration, but this extension is to be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and only in cases where it is proper and reasonable to do so. No certificate is to be extended for more than three months.

2.2.3.2 The period of validity of the interim ISSC is not to be extended.

2.2.3.3 If the Society has the sufficient reasons to determine that one of the purposes for the Company or ship to apply for continuous issuance of interim ISSCs is to avoid its responsibility for implementation of Chapter XI-2 of SOLAS Convention and ISPS Code,

the continuous issuance of interim ISSC certificates will not be granted by the Society.

#### 2.2.4 Invalidation and withdrawal of ISSC certificate

##### 2.2.4.1 A certificate becomes invalid or is to be withdrawn in any of the following cases:

- (1) Intermediate verifications is not carried out as specified in Chapter 4 of the Guidelines in the specified period of time;
- (2) additional verification required by the society and Administration is not completed within the specified period;
- (3) when corrective and preventative actions against the failures identified during verification have not been completed within the specified period;
- (4) the major failures identified during shipboard verification cannot be downgraded before ailing
- (5) the Company ceases to operate the ship or the ship has been out of service.;
- (6) when the ship security plan is amended without approval by the Society;
- (7) when the ship security system has not been in actual operation for more than six months.
- (8) Payment of certification fees is not made in time and no appropriate action is taken either.

2.2.4.2 When the Society has sufficient reasons to determine the invalidation or cancellation of the certificate, the Society will notify in writing the Company which the ship serves and the flag Administration of the information of the involved ship and Company and the reasons for doing so.

2.2.4.3 When the Society cancels an ISSC under the authorization of the flag Administration, the Society will notify in writing the Company managing the ship or the ship master, and in all cases, the Company shall ensure the ship is informed that the ISSC has been cancelled as of the signature date of the notification and request the ISSC to be returned. A copy of such notification is to be sent to the flag Administration, Administration of the Port State (where applicable) and the classification society by which the ship was classed. When the Company managing the ship ceases management of that ship, the Company is to notify the Society immediately and return the ISSC.

#### 2.2.5 Retention, Reissue, Revisions and Return of Certificates

##### 2.2.5.1 Retention of certificate

The certificate is to be retained onboard the ship, and the copy of the certificate is to be retained in the Company. They are to be presented upon the Society's request.

##### 2.2.5.2 Re-issue of certificate

- (1) Application for re-issuing an ISSC certificate is to be submitted by the Company to the Society without delay in case of its ISSC certificate being lost or damaged.
- (2) After invalidation or withdraw of the certificate mentioned in 2.2.4.1 (1), (2), (3), (4), (6) and (8), only when d an additional verification is carried out with the same scope and extent as the initial verification, can ISSC be re-issued. The validity of the new certificate is to be the same as that of the invalidated or canceled one.

##### 2.2.5.3 Revision of certificate

Whenever the content of the certificate is changed, the Company is to promptly apply to

the Society for revising and re-issue the certificate.

#### 2.2.5.4 Return of certificate and document

The Company is to return the certificate immediately to the Society in any of the following cases:

- (1) when new ISSC is issued in accordance with 2.2.1;
- (2) when the certificate is re-issued after has been withdrawn or invalidated;
- (3) Where the lost original certificate is found after it is reissued, the original one is to be immediately returned to the society.

## **Chapter 3 APPROVAL OF SHIP SECURITY PLAN**

### **Section 1 General Requirements**

- 3.1.1 The application for approval of ship security plan is to be submitted by the Company which the ship serves to the Headquarters of the Society or the unit designated by the Society.
- 3.1.2 During the verification of ship security system carried out in accordance with Chapter 4 of the Guidelines, the Society will not accept the application for amendments to the ship security plan (SSP) not approved by the Society.
- 3.1.3 For the review of the documents related to ship security, the Society is to determine:
- (1) that ship security assessment (SSA) has been carried out, and is in compliance with the requirements of ISPS Code;
  - (2) that the preparation of ship security plan (SSP) and its amendments are based on ship security assessment, and are in compliance with three security levels defined in ISPS Code.
- 3.1.4 When authorized by the flag Administration, the Society will approve the ship security plan (SSP) on behalf of the flag Administration.

### **Section 2 Documents to be Submitted**

- 3.2.1 The Company is to submit one copy of each of the following documents to the Society for examination about the application for the approval of ship security plan by the Society:
- (1) a duplicated copy of DOC;
  - (2) ship security plan;
  - (3) report of ship security assessment on which the ship security plan is based.
- Note: Paper or electronic format can be adopted for the documents.
- 3.2.2 The relevant documents are to be submitted if the following are not included in the ship security plan :
- (1) organizational structure and procedures for describing specific responsibilities and authority of company security officer (CSO) and other shore-based personnel related to ship security;
  - (2) company's declaration for describing that the Company is to provide CSO and master with necessary support so as to ensure the fulfillment of their responsibilities related to security.
- 3.2.3 The Company is to submit to the Society the evidence information that the company security officer (CSO) has received necessary training for implementing his responsibilities.
- 3.2.4 If considered necessary by the Society, it may require the Company submitting other documents related to ship security system as supplement to those required above.

### **Section 3 Ship Security Plan**

- 3.3.1 Ship Security Plan (SSP) is to be written in working language(s) of the ship or the

language understood by the crew. If the language used is not English, French or Spanish, at least a translation into English is also to be submitted.

- 3.3.2 Ship security plan is to be developed on the basis of the ship security assessment and to be in compliance with the relevant requirements in Part A of ISPS Code, as appropriate, taking into account the guidance given in 8.1 to 13.8 of Part B of the ISPS Code.
- 3.3.3 Ship security assessment (SSA) is to be in compliance with the relevant requirements in Part A of ISPS Code, and is to ensure that:
- (1) the ship security assessment is to be carried out by persons with appropriate skills to evaluate the risk and problems of the security of a ship;
  - (2) it is to be carried out on the basis of specific threat scenarios , including regular trade patterns, with consideration of the ship’s vulnerabilities and the consequence of these scenarios;
  - (3) the guidance is fully taken into account as given in 8.1 to 13.8 of Part B of ISPS Code.
- 3.3.4 Where the Company submits a general ship security plan covering part or whole of its fleet, the Society will accept such a plan only when there is evidence that the Company has carried out the ship security assessment including on-scene security survey for each ship and that the ship security assessment and submitted ship security plans reflect the ship-specific information accurately for each ship. The Society will act in accordance with the provisions specified by the Administration when conducting review and approval of ship security plans on its behalf.

#### **Section 4 Review of Documents**

- 3.4.1 Upon request by the Company, the qualified maritime security auditor (hereinafter referred as “the auditor”) of the Society, as appropriate, is to carry out the review of the documents.
- 3.4.2 Findings of the document review are to be documented in a clear and concise manner and supported by objective evidence. The auditor is to prepare the review report for the ship security plan based on the information gathered.
- 3.4.3 . When reviewing and approving a SSP, the auditor shall verify that the Company has taken into account relevant security-related guidance and best management practices, including the latest IMO Circulars concerning piracy, hijacking and armed robbery. If the Society considers that the ship security plan and the ship security assessment are not in compliance with the appropriate verification criteria (1.3.3), the Company is required to revise them appropriately and resubmit them for review.
- 3.4.4 Upon review, if the ship security plan is considered to be in compliance with ISPS Code A/9.4 taking into account the guidance given in ISPS Code B/8.1 to 13.8 and is appropriate for the ship, the Society will approve the ship security plan and issue a Letter of Approval for the ship security plan.
- 3.4.5 The ship security plan is to be affixed with an business stamp on every pages to avoid the unauthorized revision and is to be returned to the Company together with the Letter of Approval. The ship security plan is to be kept onboard the ship.
- 3.4.6 There shall be evidence indicating that the company security officers (CSOs) have received training in accordance with A/13.1 under ISPS Code. If the company cannot

provide evidence or there is objective evidence showing that the CSOs have not received the prescribed training, the auditor is to notify the Company so that corrective actions can be taken.

### **Section 5 Approval for Amendments to the Approved Ship Security Plan**

- 3.5.1 Any amendments in accordance with the requirements under A/9.4.1 to A/9.4.18 of ISPS Code made to the ship security plan approved by the Society is to be submitted to the Society for review and approval.
- 3.5.2 When applying for approval of amendments to the ship security plan, the Company is to submit the following documents:
- (1) the amended cover, contents of the ship security plan or the list of the documents, amendment record;
  - (2) relevant documents of the ship security plan prior to amendment (duplicated copies are accepted);
  - (3) relevant documents of the ship security plan after amendment;
  - (4) report of the ship security assessment resulting in the amendment of the ship security plan.
- 3.5.3 If the amendments to the ship security plan is considered to be in compliance with the verification criteria after the review of amendments to the relevant documents of the ship security plan, the Society is to affix approval stamp to the relevant documents of the amended ship security plan, and return them to the Company. The Company is to ensure the renewal of the ship security plan onboard the ship.
- 3.5.4 In accordance with the extent and nature of the amendments to the ship security plan, the Society is to determine whether an additional verification is required, and notify the Company of the decision. The amendments to the ship security plan due to the installation or replacement of the ship security alert system are to be subject to an additional verification.

## Chapter 4 AUDIT OF SHIP SECURITY SYSTEM

### Section 1 General Requirements

#### 4.1.1 Application

4.1.1.1 The ship requesting audit by the Society is to submit an application to the Society.

#### 4.1.2 The requirements for the Company and/or the ship

4.1.2.1 The Company is to hold a Document of Compliance (DOC) of the company safety management system and the Safety Management Certificate of the ship accepted by the Society

4.1.2.2 The Company is to provide the documented ship security assessment (SSA), security procedures and associated records carried out or made by the company security officer or persons with appropriate skills authorized by him. These records are to provide objective evidence for the implementation of ship security plan (SSP) and the maintenance of any security equipment specified in the ship security plan. When applying for initial audit by the Society, the Company is to ensure that sufficient objective evidence is available for the implementation of the security system of the ship.

4.1.2.3 The Company shall carry out both internal audits and reviews of security activities at least once every twelve (12) months onboard each ship applying for certification, and provide appropriate evidence to prove it.

4.1.2.4 The Company is to ensure the appropriate investigation and analysis of the failures identified during the audit and take corrective actions.

4.1.2.5 The audit of the compliance of ship security system by the Society will not reduce the obligations of the Company and all the crew to abide by national and international laws, or the security levels of the areas where they work or carry out their business activities.

4.1.2.6 The Company and the ship are to maintain records of their internal and external security verifications for a minimum period of five years.

4.1.2.7 Any amendments made to the security system, the security equipment or the SSP and that are related to the requirements of ISPS Code A/9.4.1 to A/9.4.18, must be submitted to the Society for review and approval.

4.1.2.8 At the initial installation of the SSAS, the Company shall arrange an approved Radio Technician to test and issue a report on the equipment's compliance with the requirements of SOLAS XI-2/6.2 to 6.4. A SSAS-SC may be tested and reported by the SSO.

4.1.2.9 Following the initial installation of SSAS, the Company is responsible for:

- (1) testing and maintaining the SSAS to satisfy operational requirements according to the approved SSP; and
- (2) maintaining on board the SSAS records specified in A/10.1.10 of ISPS Code.

#### 4.1.3 Preparations and implementation of the audit

4.1.3.1 Upon the Company's application, a qualified maritime security auditor (hereinafter referred to as "the auditor") of the Society, is to carry out the verification.

4.1.3.2 During the audit, the Company is to arrange for a person who is familiar with audit

- procedures and who is capable of preparing audit work to assist the auditor when required.
- 4.1.3.3 The Company whose ship is to be audited is to make necessary preparation in accordance with the audit plan notified by the Society in advance and the requirements (if any) of the auditor. The preparation for the audit is to ensure that the auditor has access to all the documents, records related to the ship security system during the audit
- 4.1.3.4 The audit can be suspended if the Company has not made sufficient preparation for the audit or does not designate persons to receive the audit, or if the auditor considers it difficult to continue the audit.
- 4.1.3.5 Only when the ship is under normal operation condition and with full complement of crew onboard in accordance with the Safely Manning Certificate, can the initial verification, periodical verification and additional verification mentioned in 4.1.6 be carried out.
- 4.1.3.6 Audits for the issue or renewal of ISSCs shall consist of the following steps:
- (1) verification that an approved SSP is onboard;
  - (2) verification through a representative sample that the security system is being implemented effectively;
  - (3) verification that all security equipment specified in the SSP complies with applicable requirements;
  - (4) verification that all security equipment specified in SSP, including the ship security alert system, is operational.
- 4.1.3.7 The auditor is to hold an opening meeting with the master and/or senior management of the ship before the beginning of the verification , so as to :
- (1) Introduce auditors to the ship management;
  - (2) explain the scope and purpose of the audit;
  - (3) provide a short summary of the methods and procedures to be used;
  - (4) establish the official communication line between the auditor and the shipboard management;
  - (5) confirm that the necessary resources, documentation and facilities are available;
  - (6) confirm dates and time of the closing meeting and any interim meetings.
- 4.1.3.8 Upon completion of the audit, a closing meeting is to be held to present the audit findings and the handling requirements for deficiencies to the master and/or the senior management of the ship, and audit conclusions will be announced by the lead auditor.
- 4.1.3.9 The auditor shall verify the effective implementation of the approved SSP and its documented procedures based on objective evidence obtained by interviews, inspections, review of documents and examination of records.
- 4.1.3.10 All the technical security equipment or systems specified in the ship security plan is to be verified. Operational security measures may be verified through sampling. After initial installation of SSAS, the society may approve the related provisions in the SSP, and verify, by audit and the witnessing of a complete security alert test, the effective implementation of those provisions.. At each subsequent scheduled audit the auditor shall examine the records of the testing of the SSAS, identify the SSAS activation points and verify the effective implementation of the procedures, instructions and guidance relating to the SSAS.
- 4.1.3.11 The auditor may ask for information from any other RSO or, if relevant the Administration, in order to check the accuracy of the information provided by the

Company.

4.1.3.12 Intermediate and renewal audits shall include a review of Failures reported following previous audits. The auditor shall select a sample of the reported Failures and verify that the company is investigating, analyzing and resolving them effectively and in a timely manner.

4.1.4 Audit findings

4.1.4.1 The audit findings are to be documented in a clear and concise manner and supported by objective evidence. Audit findings shall be reviewed by the auditor(s) in order to determine whether they should be reported as Major Failures, Failures or Observations and should be communicated to the representative of the Company and/or the ship's senior management so that they can recognize and take corrective actions.

4.1.4.2 Failures shall be raised against the corresponding requirement of the ISPS Code, the relevant sections or paragraphs of the SSP and any specific Flag State requirements.

4.1.4.3 An ISSC is not to be issued or renewed if a Major Failure exists at initial and renewal audits. Such finding shall be reported immediately to the flag administration and immediate action is required to restore compliance.. The auditor shall verify the implementation of these measures and requirements from the flag administration (if any) before the ship sails. A schedule for the implementation of actions to prevent recurrence shall be agreed between the Company and the auditor to prevent recurrence. At least one additional audit shall be carried out within the period agreed for the verification of implementation of the actions to prevent recurrence.

4.1.4.4 An ISSC shall not be endorsed if a Major Failure exists at intermediate audits. Immediate action is required to restore compliance, thereby permitting the Major Failure to be down-graded. The auditor shall verify the implementation of these measures before the ship sails and a schedule for the implementation of actions to prevent recurrence shall be agreed between the Company and the auditor. At least one additional audit shall be carried out within the period agreed for the verification of implementation of the actions to prevent recurrence.

4.1.4.5 An ISSC shall not be issued or renewed until all identified failures have been resolved and compliance has been restored. In addition, a schedule for the implementation of actions to prevent recurrence need to be agreed between the Company and the auditor. Additional audits may be carried out as necessary.

4.1.4.6 An ISSC may be endorsed following identification of a Failure at intermediate and additional audits, provided that compliance has been restored, or a schedule has been agreed between the Company and the auditor for the completion of corrective action to restore compliance and to prevent recurrence. Additional audits may be carried out as necessary.

4.1.4.7 Additional audit carried out for the major failures identified during audit and failures that require follow-up verification is to be completed within three (3) months starting from the completion date of the audit.

4.1.5 Audit report

4.1.5.1 A report is to be produced after every SSP approval and audit, and a copy of such

report must be retained on board.

4.1.5.2 An audit report is to be prepared by the auditor based on the audit findings gathered and the compliance of the ship security system with the approved ship security plan and ISPS Code.

4.1.5.3 The audit report is to be accurate and complete, and shall include following items:

- (1) the date and time of completion of the audit.
- (2) the status of the implementation of the SSP.
- (3) confirmation of the operational status of all security equipment and systems on board.
- (4) reports of any failures found during the audit.

4.1.6 Type of verification

4.1.6.1 The verification of the ship security system consists of the following types:

- (1) initial verification
- (2) periodical verification:
- (3) intermediate verification / renewal verification
- (4) additional verification
- (5) interim verification

## **Section 2 Initial Verification**

4.2.1 General requirements

4.2.1.1 When the Society verifies the ship security system in accordance with the approved ship security plan for the first time, the initial verification is to be carried out.

4.2.1.2 During initial verification, the Society is to check the documents (hereinafter referred to as “document check”) specified in 4.2.2 before carrying out the site verification so as to ensure the effective implementation of the ship security system onboard the ship (hereinafter referred to as “shipboard verification”).

4.2.2 Document check

4.2.2.1 If the ship security plan of the ship applying to the Society for initial verification is approved by the Society, the auditor is to check the ship security plan, as appropriate, during or prior to the onboard verification.

4.2.2.2 If the ship security plan of the ship applying to the Society for initial verification for issuing ISSC is approved not by the Society, the Society may require the Company to submit the copy of the approved SSP and the relevant information of the ship security assessment prior to the verification implementation.

4.2.2.3 In the cases mentioned above, if the ship security plan is considered not in compliance with the verification criteria (1.3.3), the Society is to notify this in writing to the Company and the flag Administration.

4.2.3 Shipboard verification

4.2.3.1 The Society is to determine whether the ship security system is in full compliance with the requirements of the verification criteria (1.3.3), is in satisfactory condition and is

appropriate to the expected operation of the ship through onboard verification.

4.2.3.2 The following security activities are at least to be covered by shipboard verification:

- (1) organization of the ship security and the fulfillment of the security responsibilities, including company security officer, master, ship security officer and all other persons with security responsibilities onboard the ship, and necessary support provided by the Company;
- (2) control methods and measures for access to ship;
- (3) control of the embarkation of persons and their effects (accompanied and unaccompanied baggage);
- (4) surveillance and monitoring of the restricted areas to ensure that only authorized persons have access;
- (5) monitoring of deck areas and areas surrounding the ship;
- (6) control of the handling of cargo and the delivery of ship's stores;
- (7) response to the change of the security levels by the ship;
- (8) completion of a Declaration of Security, including interface with any port facility and/or ship to which Chapter XI-2 of SOLAS and ISPS Code are not applicable;
- (9) response to the threats or breaches of security, including personnel evacuation;
- (10) report and handling of security incidents;
- (11) operation of ship security communication equipment or system and control of security information;
- (12) status, maintenance, test, calibration and use of all the security equipment and/or system;
- (13) training of the personnel onboard the ship, security drills and exercises;
- (14) internal audit and review of the security activities onboard the ship and review of and amendments to the ship security plan;
- (15) control of the sensitive information;
- (16) control of the records of the ship security activities;
- (17) checking the records of statutory surveys related to ship security alert system (SSAS), automatic identification system (AIS) and checking the conformity of actual marking of the ship identification number with that mentioned in the document including continuous synopsis record (CSR).

4.2.3.3 Upon the satisfactory completion of the initial verification and upon the authorization of the flag Administration, the Society is to issue an ISSC with validity not exceeding five (5) years. A certificate of shorter validity may be issued in accordance with this Society procedures and flag State requirements.

### **Section 3 Periodical Verification**

4.3.1 General requirements

4.3.1.1 The ship with ISPS certification by the Society is to accept periodical verification specified in this Section so as to keep the ISSC certificate valid.

4.3.1.2 The Company has the responsibility to apply to the Society for periodical verification so as to keep the certificate valid, and is to get ready in accordance with relevant requirements.

- 4.3.2 Intermediate verification
- 4.3.2.1 During intermediate verification, the Society is to determine on board the ship whether the ship security system is maintained in compliance with the approved ship security plan and to be continuously appropriate to the expected service of the ship.
- 4.3.2.2 The intermediate verification is to be carried out between the second and third anniversary date of ISSC certificate.
- 4.3.2.3 The items of the intermediate verification is generally the same as those of initial verification (4.2.3.2), and the effectiveness of the corrective actions taken for any non-conformity found during the last audit is to be verified.
- 4.3.2.4 Any failure of the ship security system found during verification is to be handled in accordance with 4.1.4.
- 4.3.2.5 After the satisfactory completion of the intermediate verification, the ISSC shall be endorsed by the auditor.
- 4.3.3 Renewal verification
- 4.3.3.1 During renewal verification, the Society is to determine on board the ship whether the ship security system is in full compliance with the approved ship security plan and in satisfactory condition, and to be appropriate to the expected service of the ship.
- 4.3.3.2 The renewal verification is to be completed at the interval of not more than 5 years and within three (3) months prior to the expiry date of the existing certificate, except for those cases mentioned in 2.2.3.1.
- 4.3.3.3 The items of the renewal verification is generally the same as those of initial verification (4.2.3.2), and the effectiveness of the corrective actions taken for any non-conformity found during the last audit is to be verified.
- 4.3.3.4 After satisfactory completion of the renewal verification, the Society will issue an ISSC or endorse for extension on the existing certificate.

#### **Section 4 Additional Verification**

- 4.4.1 The Society is to carry out additional verification in the following cases:
- (1) major influence of the substantial changes of the ship security plan to the operation of the ship security system;
  - (2) any non-conformity as mentioned in 4.1.4.2 and 4.1.4.3 exists;
  - (3) any non-conformity as mentioned in 4.1.4.4 and 4.1.4.5 exists and additional audit is required by the Society;
  - (4) if required by the flag Administration;
  - (5) major security incident of the ship taking place;
  - (6) any non-conformity of the ship security resulting in the ship being detained, expelled from the port, its entry into port refused or other operation limits, and required by relevant port authorities;
  - (7) change of the names of the ship, company and registered place, class and other conditions the Society considers.
- 4.4.2 The scope and extent of the additional verification are to be determined by the Society in accordance with the nature of the additional verification or the requirements by the flag

Administration.

- 4.4.3 Any failure of the ship security system found during the verification is to be handled in accordance with 4.1.4.2 and 4.1.4.3.
- 4.4.4 After the satisfactory completion of the additional verification, the certificate is to be endorsed.
- 4.4.5 Actions to be taken after PSC detention
  - 4.4.5.1 If the ship is detained due to ISPS deficiency, the Company shall inform the Society and apply for an additional audit from the Society.
  - 4.4.5.2 All failures must be handled in accordance with relevant requirements as mentioned above in 4.1.4.
  - 4.4.5.3 If the auditor disagrees with the conclusions of the duly authorized officer, the reasons for the disagreement shall be documented in the audit report. The duly authorized officer, the Company and the Administration must be made aware of the auditor's comments in this respect.

## **Section 5 Interim Verification**

- 4.5.1 The ship may apply for the verification for issuance of interim ISSC in one of the following cases:
  - (1) a ship without a certificate, on delivery or prior to its entry or re-entry into service;
  - (2) transfer of a ship from the flag of an Administration to the flag of another Administration, including the transfer of the Administration of a ship from the non-contracting one to the contracting one; or
  - (3) when a company assumes the responsibility for the operation of a ship not previously operated by that Company.
- 4.5.2 For the purpose of the issuance of an interim ISSC, the Society is to verify the following:
  - (1) the ship security assessment has been completed;
  - (2) a copy of the ship security plan is provided and implemented on board the ship, and the original plan has been submitted for review and approval;
  - (3) the ship is provided with a ship security alert system as required, if any;
  - (4) the security officer is assigned to the ship as required;
  - (5) the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities and with the relevant provisions of the ship security plan placed on board; and such information related to ship security have been provided onboard which is written in the working language of the ship's personnel or language(s) understood by them;
  - (6) the company security officer has ensured:
    - a. the review of the ship security plan for compliance with Part A of the ISPS Code;
    - b. that the plan has been submitted for approval; and
    - c. that the plan is being implemented on the ship;
  - (7) evidence of arrangements for drills, exercises and for internal audit by the Company within next three (3) months, including the plan for completion of an initial verification required by the ISPS Code within next six (6) months.

Annex 1: ISPS Code certification scenarios – minimum requirements

**ISPS CODE CERTIFICATION SCENARIOS – MINIMUM REQUIREMENTS**

	<b>Scenario</b>	<b>Condition</b>	<b>Action required</b>	<b>Ship Security Plan</b>	<b>Scope of Audit and Certification</b>
<b>1</b>	Change of ship's name/Port of Registry/Gross Tonnage.	Conducted by a surveyor or an auditor	Verification on board (Change of ship's name) or Verification at office (Change of ship's Port of Registry/Gross Tonnage)	1. Verify correct ship's name/Port of Registry/Gross Tonnage on the title page, index page and revision page of SSP. 2. Amend/reissue SSP Approval Letter with the ship's new name/Port of Registry/Gross Tonnage.	1. Verify correct ship's name/Port of Registry/Gross Tonnage on all Certificates and Documents. 2. Verify that SSAS has been reprogrammed with the ship's new particulars. 3. Amend/reissue ISSC with the ship's new name/Port of Registry/Gross Tonnage. <i>Note:</i> ISSC must be amended by issuing organization or by special arrangement <sup>1</sup> . Replacement ISSC shall have the same expiry date as the current ISSC.
<b>2</b>	Change of flag	Conducted by an auditor	Interim audit on board	1. Check that the SSP is on board. 2. Check that SSP addresses ISPS Code A/9.4.1 to A/9.4.18. 3. Check that a copy of the SSP has been submitted to the Administration or its organization for approval.	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
		1. SSP has already been approved for the new flag 2. Conducted by an auditor	Additional audit on board		1. Verify compliance with the requirements of the SSP and reprogramming of SSAS. 2. Issue a replacement ISSC with same expiry date as the current ISSC.
<b>3</b>	Change in IMO ship type	Conducted by an auditor	Interim audit on board	Verify amendments to SSP, if any, have been submitted for approval	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC with new ship type.
<b>4</b>	Takeover of certification from an organization not subject to verification of compliance with QSCS in accordance with	Conducted by an auditor	Initial audit on board		1. Audit to address all elements of ISPS Code. 2. Issue ISSC.

	<b>Scenario</b>	<b>Condition</b>	<b>Action required</b>	<b>Ship Security Plan</b>	<b>Scope of Audit and Certification</b>
	Section 5 of Annex 1 to the QSCS				
<b>5</b>	Ship out of service between 3 and 6 months <sup>2</sup>	Conducted by an auditor	Additional audit if re-quired by the Administration		Endorse ISSC as appropriate.
<b>6</b>	Ship out of service more than 6 months <sup>2</sup>	Conducted by an auditor	Interim audit on board		1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
<b>7</b>	Intermediate audits requested after the end of the audit time window	Conducted by an auditor	Intermediate audit on board		1. If reinstated, ISSC to be endorsed with a statement (e.g. Validity reinstated with scope as initial). If re-issued, ISSC to have same expiry date as previous certificate. 2. Issue PR17 report if ISM audit is not held at the same time.
<b>8</b>	Change of Company name and/or address		Attendance on board not required	1. Approve SSP amendments to reflect new Company name and address. 2. Reissue approval letter.	1. Verify DOC has been reissued with new Company name and address. 2. Issue replacement ISSC with same expiry date as previous ISSC.

Note: Above scenarios may be subject to flag State requirements and should only be applied in the absence of any instructions from the Administration.

<sup>1</sup> The organization may with permission from the Administration authorize a surveyor from the vessel's Classification Society, if other than the ISPS organization, to amend the documentation.

<sup>2</sup> These instructions do not apply to ships for which seasonal lay-ups are a normal part of their operational routine – refer to MSC-MEPC./7 Circ.9.

**International Ship Classification  
INTERNATIONAL SHIP SECURITY CERTIFICATE**

Certificate No. \_\_\_\_\_

**Issued under the provisions of the  
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES  
(ISPS CODE)**

Under the authority of the Government of \_\_\_\_\_  
*(name of State)*

by International Ship Classification.

Name of ship: .....  
Distinctive number or letters: .....  
Port of registry: .....  
Type of ship: .....  
Gross tonnage: .....  
IMO Number: .....  
Name and address of Company: .....  
Company identification number: .....

**THIS IS TO CERTIFY:**

- 1 that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of Part A of the ISPS Code;
- 2 that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complied with the applicable requirements of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code;
- 3 that the ship is provided with an approved Ship Security Plan.

Date of initial/renewal verification<sup>1</sup> on which this certificate is based.....

This Certificate is valid until ....., subject to verifications in accordance with section 19.1.1 of Part A of the ISPS Code.

Issue at .....  
*(Place of issue of the Certificate)*

Date of issue .....

*(Stamp of ISC)*

.....  
International Ship Classification

\_\_\_\_\_  
<sup>1</sup> Delete as appropriate.

**ENDORSEMENT FOR INTERMEDIATE VERIFICATION**

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of Part A of the ISPS Code the ship was found to comply with the relevant provisions of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

Intermediate verification  
*(Stamp of ISC)*

Signed .....  
*(Signature of ISC auditor)*  
Place .....  
Date .....

**ENDORSEMENT FOR ADDITIONAL VERIFICATIONS<sup>1</sup>**

Additional verification  
*(Stamp of ISC)*

Signed .....  
*(Signature of ISC auditor)*  
Place .....  
Date .....

Additional verification  
*(Stamp of ISC)*

Signed .....  
*(Signature of ISC auditor)*  
Place .....  
Date .....

Additional verification  
*(Stamp of ISC)*

Signed .....  
*(Signature of ISC auditor)*  
Place .....  
Date .....

---

<sup>1</sup> This part of the certificate shall be adapted by the Administration to indicate whether it has established additional verifications as provided for in section 19.1.1.4.

**ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF THE ISPS CODE**

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of Part A of the ISPS Code the ship was found to comply with the relevant provisions of Chapter XI-2 of the SOALS Convention and Part A of the ISPS Code.

Signed .....  
(Signature of ISC auditor)  
Place .....  
Date .....

**ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of Part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of Part A of the ISPS Code, be accepted as valid until .....

Signed .....  
(Signature of ISC auditor)  
Place .....  
Date .....

**ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/19.3.4 OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of Part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of Part A of the ISPS Code, be accepted as valid until .....

Signed .....  
(Signature of ISC auditor)  
Place .....  
Date .....

**ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL  
REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF ISPS CODE  
APPLIES OR FOR A PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS  
CODE APPLIES**

The Certificate shall, in accordance with section 19.3.5/19.3.6<sup>1</sup> of Part A of the ISPS Code, be accepted as valid until .....

Signed .....  
(*Signature of ISC auditor*)  
Place .....  
Date .....

(*Stamp of ISC*)

**ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION  
A/19.3.7.1 OF THE ISPS CODE APPLIES**

In accordance with section 19.3.7.1 of Part A of the ISPS Code, the new expiry date<sup>2</sup> is .....

Signed .....  
(*Signature of ISC auditor*)  
Place .....  
Date .....

---

<sup>1</sup> Delete as appropriate.

<sup>2</sup> In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

**International Ship Classification**  
**INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE**

Certificate No. \_\_\_\_\_

**Issued under the provisions of the**  
**INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES**  
**(ISPS CODE)**

Under the authority of the Government of \_\_\_\_\_  
*(name of State)*

by International Ship Classification.

Name of ship: .....  
Distinctive number or letters: .....  
Port of registry: .....  
Type of ship: .....  
Gross tonnage: .....  
IMO Number: .....  
Name and address of Company: .....  
Company identification number: .....  
Is this a subsequent, consecutive interim certificate? Yes / No<sup>1</sup>  
If Yes, date of issue of initial interim certificate .....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until .....

Issued at .....  
*(Place of issue of the certificate)*

Date of issue .....

*(Stamp of ISC)*

.....  
International Ship Classification

<sup>1</sup> Delete as appropriate.