No.24 Procedural Requirements for ISPS Code Certification

(Rev.0 July 2009) (Rev.1 Dec 2010) (Rev.2 May 2019)

Introduction

This document provides the Classification Societies with the methods and criteria for carrying out Ship Security Plan (SSP) approvals and for issuing International Ship Security Certificates (ISSCs) to ships following verification by audit that their security systems and any associated security equipment comply with the requirements of the ISPS Code and the provisions of the corresponding approved SSPs.

The Classification Societies may conduct approvals of SSPs or amendments thereto and verification of SSPs necessary for issuing an ISSC on behalf of Administrations. Certificates will comply with the format required by the Administrations.

Note:

1. This Procedural Requirement applies from 1 July 2009.

2. Rev.1 of this Procedural Requirement applies from 1 July 2011.

3. Rev.2 of this Procedural Requirement applies from 1 July 2019.

No.24 (cont)

1. Scope and Application

1.1 This document establishes the procedures for:

(i) review and approval of SSPs;

(ii) verification of compliance with the requirements of the ISPS Code;

(iii) issue of Interim, Initial, and Renewal ISSCs;

(iv) intermediate verification;

(v) additional verification;

(vi) withdrawal of certification.

1.2 This IACS Procedural Requirement (PR) is to be applied by Classification Societies when acting as RSOs on behalf of Administrations in the conduct of SSP approvals, audits and the issuance of certificates in accordance with the ISPS Code.

1.3 The scopes of the verifications carried out in accordance with this PR shall be restricted to the Requirements of SOLAS Chapter XI-2 and the ISPS Code Part A taking into account ISPS Code B/8.1 to B/13.8.

1.4 For minimum requirements relating to non-routine ISPS Code certification scenarios, please refer to Annex 1.

No.24 (cont)

2. Definitions

2.1 “Auditor” means a person trained, qualified and authorized in accordance with IACS Procedural Requirement 10 (PR10) to carry out SSP approval and audits.

2.2 “Convention” means the International Convention for the Safety of Life at Sea (SOLAS), 1974 as amended.

2.3 “ISPS Code” means the International Ship and Port Facility Security Code, (consisting of Part A and Part B), as adopted by the IMO.

2.4 “Ship Security Assessment” (SSA) is an activity carried out to identify possible threats to key shipboard operations and the likelihood of their occurrence and an evaluation of existing security measures and weaknesses in the infrastructure, policies and procedures.

2.5 “Ship Security Plan” (SSP) means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, the cargo, cargo transport units, ship’s stores or the ship from the risks of a security incident.

2.6 “Security System” is the system in place on board the ship which implements the procedures, documentation and required records which are examined to verify compliance with the requirements of the ISPS Code.

2.7 “Security Equipment” is equipment used in the implementation of the security measures specified in the SSP.

2.8 “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 the Port Facility Security Officer (PFSO) and the Ship Security Officer (SSO).

2.9 “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 the liaison with the CSO and the Port Facility Security Officer (PFSO).

2.10 “Security Incident” means any act or circumstance that theatens the security of a ship, a mobile offshore drilling unit, a high speed craft, a port facility, a ship/port interface or any ship to ship activity.

2.11 “Security Level” means the qualification of the degree of risk that a security incident will be attempted or will occur.

2.12 “Security Level 1” means the level for which minimum appropriate protective security measures shall be maintained at all times.

2.13 “Security Level 2” means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

2.14 “Security Level 3” means the level for which further specific protective security measures shall be maintained for a period of time when a security incident is probable or imminent, (although it may not be possible to identify the specific target).

2.15 “Regulation” means a regulation of the Convention.

No.24
(cont)

2.16 “Ship” when used in this Code, includes self propelled mobile offshore drilling units and high speed craft as defined in SOLAS Chapter XI-2/1.

2.17 “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.

2.18 “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.

2.19 “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.

2.20 “Verification” is confirmation through the evaluation of objective evidence that specified requirements have been fulfilled. (See also 2.23)

2.21 “Recognised Security Organisation” (RSO) means an organisation authorised by a Contracting Government in accordance with SOLAS Chapter X1-2/1.16. When "Classification Society" is used in this PR, it is always intended as "Classification Society acting as RSO".

2.22 “Ship Security Alert System” (SSAS) means a system installed on board, either interfaced with another radio installation or self-contained (abbreviated to SSAS-SC in this PR), 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).

2.23 “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.

2.24 Any capitalized terms used in this PR which are not defined above have the meanings given them in the Convention.

No.24 (cont)

3. Criteria for Verification

3.1 Criteria for verification of compliance with the requirements of the ISPS Code shall be in accordance with the applicable sections of the SOLAS Chapter XI-2 and the ISPS Code Part A.

3.2 A Classification Society performing verification of compliance with the requirements of the ISPS Code shall meet the requirements of MSC/Circ. 1074 Appendix 1, paragraphs 3 to 5.

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

3.4 A Classification Society that approves a SSP or issues an ISSC shall have implemented a documented system for the:

a) qualification and continuous updating of the knowledge and competence of auditors who perform such approvals or verifications in compliance with PR10, and

b) performance of the processes involved in accordance with this PR. This system shall, inter alia, include procedures and instructions for the following:

   (i) the establishment of contract agreements with Companies in respect of their ships;

   (ii) the scheduling and performance of SSP approvals and verifications;

   (iii) the reporting of the results of SSP approvals and verifications;

   (iv) the issue of interim and full term ISSC certificates.

3.5 Only auditors who are qualified as required by PR10 shall carry out approvals and verifications.

3.6 The entire SSP approval and implementation audit process shall verify:

   (i) that the SSP and any amendments are appropriate to the three security levels defined by the ISPS Code;

   (ii) that the SSP is complaint with the ISPS Code;

   (iii) that the SSP is being effectively implemented on board.

No.24 (cont)

4. Obligations of the Company

4.1 Where the verification of an SSP is to be carried out by a Classification Society that did not carry out the SSP approval, the Company shall provide, if requested by the Classification Society, a copy of the SSA report and the SSP prior to the audit on board.

4.2 The Company shall carry out internal audits and reviews of security activities at least once every twelve (12) months on board each ship.

4.3 The Company and the ship are to maintain records of external security verifications for a minimum period of five (5) years.

4.4 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 Classification Society for review and approval.

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

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

(i) testing and maintaining the SSAS to satisfy operational requirements according to the approved SSP; and

(ii) maintaining on board the SSAS records specified in ISPS Code A/10.1.10.

No.24 (cont)

5. Ship Security Plan Approval

5.1 The Company is to prepare and submit to the Classification Society a SSP for each ship. This SSP is to be reviewed and approved on behalf of the Administration.

5.2 Unless otherwise specified by the Administration, all changes to an approved SSP related to the requirements of ISPS Code A/9.4.1 to A/9.4.18 shall be reviewed and approved before implementation by the Classification Society that approved the SSP. The SSP and the amendments are to be accompanied by the SSA from which they were developed.

5.3 The SSP shall be developed in accordance with the requirements of ISPS Code Part A taking into account ISPS Code B/8.1 to B/13.8, and shall be written in the working language, or working languages, of the ship. If the language, or languages, used is not English, French or Spanish, a translation into one of these languages shall be included. The Classification Society undertaking the approval shall consider at least the version of the SSP written in English, French or Spanish.

5.4 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.

5.5 When the Classification Society approves the SSP and any amendments it should retain, as a minimum, a copy of the letter of approval. The evidence of this approval shall be kept on board. Marking of SSPs, following first approval and approval of amendments, shall be handled in accordance with the Classification Societies internal procedures.

5.6 The Classification Society that approves an amendment to an SSP shall determine whether any additional verification is required relating to its implementation.

5.7 During the certification period, no Classification Society shall approve amendments to a SSP approved by another Classification Society or an Administration.

5.7bis If the ISPS certification is transferred in accordance with IACS PR 18 and if the gaining Society is requested to approve any amendments to the SSP by the management company, the gaining Society shall re-approve the entire SSP.

5.8 Evidence should be sought that the Company Security Officer (CSO) has received training in accordance with ISPS Code A/13.1. If evidence is not provided by the Company or if there is objective evidence that the CSO has not received such training, the auditor should inform the Company so that corrective actions can be taken.

No.24 (cont)

6. Audit of Ships

6.1 Audits for the issue or renewal of ISSCs shall consist of the following steps:

(i) verification that an approved SSP is on board;

(ii) verification through a representative sample that the security system is being implemented effectively;

(iii) verification that all security equipment specified in the SSP complies with applicable requirements;

(iv) verification that all security equipment specified in the SSP, including the ship security alert system (SSAS), is operational.

6.2 Initial, Intermediate and Renewal audits shall be performed only under normal operating conditions and when the ship is fully manned in accordance with the Safe Manning Certificate.

6.3 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.

6.4 Following the initial installation of the SSAS, the Classification 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. Confirmation that the SSAS complies with the requirements of paragraphs 2 to 4 of SOLAS Chapter XI-2 will be found in the Radio Technician's report (or the SSO's report, in the case of a SSAS-SC).

6.5 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 as specified in ISPS Code A/9.4.18.

6.6 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.

6.7 The auditor has the authority to ask for information from any other Classification Society or, if relevant the Administration, in order to check the accuracy of the information provided by the Company.

6.8 Where the audit of a ship is to be carried out by a Classification Society that did not carry out the SSP approval, the Classification Society may review the SSP either at, or prior to, the audit on board.

No.24 (cont)

7. Failures and Corrective Action Follow-up

7.1 Audit findings shall be reviewed by the auditor(s) in order to determine whether they should be reported as Major Failures, Failures or Observations.

7.2 At the end of the Audit, the auditor(s) shall hold a meeting with the senior management of the ship and those responsible for the functions concerned. The purpose is to present Major Failures, Failures and Observations to the ship's management in such a manner that they are clearly understood.

7.3 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.

7.4 An ISSC is not to be issued or renewed if a Major Failure exists. Immediate action is required to restore compliance. 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.

7.5 An ISSC shall not be issued or renewed until compliance has been restored for all identified Failures. In addition a schedule for the implementation of action to prevent recurrence may be agreed between the Company and the auditor. Additional audits may be carried out as necessary.

7.6 An ISSC shall not to be endorsed if a Major Failure exists. 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.

7.7 An ISSC may be endorsed following identification of a Failure, 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.

No.24 (cont)

8. Issuance and Endorsement of the International Ship Security Certificate (ISSC)

8.1 The ISSC shall be issued after an Initial or Renewal audit in accordance with 6.1.

8.2 The “type of ship” to be entered on the ISSC shall be selected from those defined in SOLAS Chapter XI-2/1.

8.3 The ISSC shall be endorsed at the Intermediate audit and at any additional audit required by the Administration.

8.4 On completion of the audit, an ISSC with validity not exceeding five (5) years may be issued by the auditor. A certificate of shorter validity may be issued in accordance with Classification Society procedures and flag State requirements. When the renewal audit is completed within three months before the expiry of the existing certificate, the new certificate shall be valid until a date not exceeding five years of the expiry date of the existing certificate.

8.5 If validity of the ISSC is extended in accordance with ISPS Code A/19.3.5, documentary evidence of Administration approval must be sighted by the Classification Society.

8.6 At the request of the Company, the expiry date of ISSC may be aligned with the expiry date on the Safety Management Certificate (SMC) provided that this does not exceed the five (5) year period specified in ISPS Code A/19.3.

No.24 (cont)

9. Opening and Closing Meetings

9.1 Shipboard verification audits shall start with an opening meeting, the purpose of which is to:

(i) introduce the auditor to the ships management;

(ii) explain the scope and purpose of the audit;

(iii) provide a short summary of the methods and procedures to be used;

(iv) establish the official communication line between the auditor and the shipboard management;

(v) confirm that the necessary resources, documentation and facilities are available;

(vi) confirm the time and date of the closing meeting and any interim meetings.

9.2 On completion of each audit, the auditor shall hold a closing meeting with the shipboard management, as appropriate, to present the findings so that they are fully understood.

No.24 (cont)

10. Reporting Plan Approvals and Shipboard Audits

10.1 A report is to be produced after every SSP approval and audit.

10.2 In the case of a SSP approval, the Letter of Approval shall include the following wording: “In the development of the Ship Security Plan, in accordance with ISPS Code A/9.4, the provisions of ISPS Code B/8.1 to B/13.8 have been duly taken into account and applied as appropriate for the ship”.

10.3 The Letter of Approval shall be given to the company and retained on board the ship, together with a copy of the audit report.

10.4 In the case of an audit, the report must include the following:

(i) the date and time of completion of the audit;

(ii) the status of the implementation of the SSP;

(iii) confirmation of the operational status of all security equipment and systems on board;

(iv) reports of any Failures found during the audit.

No.24 (cont)

11. Responsibilities Pertaining to Audits

11.1 Responsibilities of the Classification Society.

11.1.1 The Classification Society is responsible for performing the audit and certification process in accordance with this PR and relevant flag State requirements.

11.2 Responsibilities of the Auditor.

11.2.1 The auditor is responsible for:

(i) carrying out the audit effectively and efficiently;

(ii) complying with the applicable procedural and regulatory requirements;

(iii) noting in the report any obstacles to the effective conduct of the audit;

(iv) organizing any special technical assistance required to verify compliance;

(v) reporting the audit results clearly, concisely and without undue delay.

11.2.2 Auditors shall treat all the information to which they have access during the course of SSP approvals and shipboard verification audits in the strictest confidence.

No.24 (cont)

12. Withdrawal of Certification

12.1 An interim ISSC shall not be issued to a ship from which a full-term ISSC has been withdrawn.

12.2 When an ISSC has been withdrawn, a new certificate may be issued only after the successful completion of an audit of scope equivalent to an initial audit.

12.3 The new certificate shall have the same expiry date as the certificate that was withdrawn.

No.24 (cont)

13. Actions Following Port State Control Detentions

13.1 When a ship is detained and deficiencies relating to the ISPS Code are given as reasons for the detention, the Classification Society that issued the ISSC shall carry out an additional audit.

13.2 Any Failures shall be dealt with in accordance with the relevant requirements of paragraph 7 above.

13.3 If the auditor disagrees with the conclusions of the Duly Authorised Officer, the reasons for the disagreement shall be documented in the audit report. The Duly Authorised Officer, the Company and the Administration must be made aware of the auditor's comments in this respect.

Annex 1

ISPS CODE CERTIFICATION SCENARIOS – MINIMUM REQUIREMENTS

	Scenario	Condition	Action required	Ship Security Plan	Scope of Audit and Certification
1	Change of ship's name	Conducted by a surveyor or an auditor	Verification on board	1. Verify correct ship's name on the title page, index page and revision page of SSP. 2. Amend SSP Approval Letter with the ship's new name.	1. Verify correct ship's name on all Certificates and Documents. 2. Verify that SSAS has been reprogrammed with the ship's new name. 3. Amend/reissue ISSC with the ship's new name. *Note:* ISSC must be amended by issuing organization or by special arrangement[1]. Replacement ISSC shall have the same expiry date as the current ISSC.
2	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.
3	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.
4	Takeover of certification from an organization not holding a QSCS certificate	Conducted by an auditor	Initial audit on board		1. Audit to address all elements of ISPS Code. 2. Issue ISSC.
5	Ship out of service between 3 and 6 months[2]	Conducted by an auditor	Additional audit if re-quired by the Administration		Endorse ISSC as appropriate.
6	Ship out of service more than 6 months[2]	Conducted by an auditor	Interim audit on board		1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
7	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 endor-sed 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.

	Scenario	Condition	Action required	Ship Security Plan	Scope of Audit and Certification
8	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.

[1] 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.
[2] 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.

Annex 2

APPLICATION OF THE ISPS CODE TO FPSOs AND FSUs

See MSC-MEPC.2/Circ.9 of 25 May 2010 “Guidance for the application of safety, security and environmental protection provisions to FPSOs and FSUs”.

Annex 3

NOTIFICATION OF INVALIDATION OF ISPS CERTIFICATION (ISSC)

Ship's Name:	IMO No.
Company Name and Address:	Certificate No.
	Issued by:
The audit was conducted on behalf of the government of:	
Type of audit: Intermediate ☐ Additional ☐ Renewal ☐ (Tick as appropriate)	

REASON FOR INVALIDATION OF CERTIFICATION (specify):

Name:	Position:	Society:	Date:

Distribution:

- Copy to Company
- Copy to Administration
- Copy to Port State Authority (if appropriate)
- Copy to Classification Society

End of Document