Amendments to the "Rules for Shipboard Security System Certification"

Effective from 1/1/2026

List of the amendments:

Paragraph/Tables amended	Reason
INTRODUCTION, SCOPE AND APPLICATION, [10.2.2], [14.2]	to specify that confidentiality of security data held by inspectors following security inspections is also to be ensured towards third parties, and to update references to some IMO documents (Prop. 308)
Annex 1	to introduce IACS PR 24 (Rev.3 Dec 2024) "Procedural Requirements for ISPS Code Certification"

INTRODUCTION, SCOPE AND APPLICATION

These Rules provides 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.
TASNEEF 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.
These Rules establish procedures for:

a) review and approve Ship Security Plans (SSPs);

b) verify compliance with the requirements of the ISPS Code and ~~to~~ issue an International Ship Security Certificate or a Statement of Compliance for the issue of an International Ship Security Certificate to a ship, when TASNEEF is acting as a Recognised Security Organisation on behalf of a SOLAS Convention Contracting Government;

c) issue a Statement of Compliance of a Shipboard Security System with these Rules when requested by a Company on voluntary basis;

d) carry out the relevant periodical verification for the maintenance of the International Ship Security Certificate (intermediate verification);

e) issue of interim, initial, renewal ISSCs;

f) additional verification;

g) withdrawal of certification.

These Rules reflect:

- the "Procedural Requirements for ISPS Code Certification" (PR24) issued by the International Association of Classification Societies (IACS).PR24 is to be applied when TASNEEF is acting as RSOs on behalf of the Administration in the conduct of SSP approvals, audits and the issuance of certificates in accordance with the ISPS Code. The scope of the verifications carried out in accordance with this PR24 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. For Minimum requirements relating to non-.routine ISPS Code certification scenarios please refer to Annex 1.
- the “Procedural Requirements for the Transfer of Safety and Security Management Systems Certification (PR18)” issued by the International Association of Classification Societies (IACS).
- IACS Recommendation No. 41 Guidance for Auditors to the ISM Code Annex 5
- MSC/~~-~~Circ.1097 “Guidance relating to implementation of SOLAS ChapterXI-2 and the ISPS Code” dated 06 June 2003.
- IACS Rec. 124 “Guidance on the Role of the Recognised Security Organization in relation to the employment of armed guards and the installation of citadels on board ships threatened by piracy in the Indian Ocean”.
- IMO Resolution MSC.147(77), Revised Performance Standards for a ship Security Alert System adopted 29 May 2003.
- IMO Circular MSC/Circ.1072, Guidance on Provision of Ship Security Alert Systems, dated 26 June 2003.
- MSC.74(69), Annex 3, Recommendation on Performance Standards for Universal Automatic Identification System (AIS), adopted 12 May 1998 and MSC.115(73), Revised Recommendation on Performance Standards for Universal Automatic Identification Shipborne Combined GPS/GLONASS Receiver Equipment, adopted on 1 December 2000~~.~~
- MSC/Circ.1074,Interim Guidelines for the authorisation of RSO acting on behalf of the Administration and/or Deisgnated Authority of a Contracting Government.

In addition to SOLAS Ch. XI-2 and the mandatory Part A of the ISPS Code, a recommendatory Part B of the same Code is intended to provide guidelines for the implementation of the mandatory requirements.

Part B of the Code will provide guidance during the verification for the Ship Security Certification.

These Rules apply to those ships operated by Companies which request security verification from RINA.

In application of these Rules, when an audit is carried out on behalf of an Administration which has appointed RINA as a Recognised Security Organisation, any rules and requirements imposed by the flag Administration are to be verified when they are different and/or more stringent than those stipulated here.

1 VERIFICATION

1.1 Definition

1.1.1 Auditor

“Auditor” means a TASNEEF exclusive employee trained, qualified and authorised in accordance with IACS Procedural Requirement 10 (PR10) to carry out SSP approval and audits.

1.1.2 Convention

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

1.1.3 ISPS Code

“ISPS Code” means the International Ship and Port Facility Security Code (ISPS) as adopted by IMO.

1.1.4 Ship Security Assessment (SSA)

“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.

1.1.5 Ship Security Plan (SSP)

“Ship Security Plan” 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 risk of a security incident.

1.1.6 Security System

“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.

1.1.7 Security Equipment

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

1.1.8 Company Security Officer (CSO)

“Company Security Officer” means the person designated by the Company for ensuring that a Ship Security Assessment is

...OMISSIS...

6.4 Where the transfer of certification occurs within the intermediate or renewal due date window, the corresponding audit may serve as the audit required in 6.3, respectively.

If the audit is successful within one month of the issue of the new certificate, the gaining society shall inform the losing society using the form provided in PR 18. If the audit is not successful within two working days, the gaining RSO shall inform the losing society by using the form attached to PR 18 (step 3 of Annex 5) and attaching the audit report in which reason for the rejection should be fully explained.

6.5 If TASNEEF receives an application from a gaining society, all information/documentation required by PR 18 of IACS shall be submitted to the gaining Society within three working days of the receipt of the completed step 1 (Annex 5) The documentation to be attached to the form by the losing RSO includes:

(i) the last external audit report, including any any failures identified;
(ii) evidence that corrective action has been proposed and the failure has been properly addressed; and
(iii) any other information that may be relevant to the decision to accept or reject the transfer of certification.

6.6 Upon receipt of information that a new certificate has been issued by the GS the LS shall issue a "Notification of Invalidation of Certification" in accordance with PR24 as applicable, ensuring that the GS is included in its circulation.

6.7 Upon receipt of information that the audit is not successful because of an unresolved failure raised by the GS, the LS shall review the findings and take action as appropriate.

7 ISM ISPS CODE AND MLC EXPIRATION DATE ALIGNMENT

7.1 When the Company selects a single RO/RSO to aligned audits:

(i) The lead auditor must be qualified for both ISM Code and ISPS Code certification and MLC, in accordance with the requirements of PR 10 and PR10B;
(ii) The RO/RSO must be authorised to conduct both the ISM Code audit the ISPS Code audit and MLC Inspection by the flag Administration;
(iii) In the case of transfer of management system certification, PR 18 and PR36 will be applicable as appropriate;
(iv) All elements of the ISM Code and/or ISPS Code MLC shall be covered in the aligned audits and inspection relative to the adjusted certificate(s);
(v) Results of the aligned audits shall be documented and reported separately and in accordance with PR 9 and PR 24 and PR40;
(vi) Any change in the expiration date of the adjusted certificate requires a full renewal verification to be carried out, unless the expiration date of the adjusted certificate(s) is moved backwards and provided that the adjustment does not circumvent any audit due or falling due at the time that the harmonisation is completed.

7.2 Upon successful completion of the alignment, the new certificate(s) shall be issued or the existing certificate(s) replaced as needed to achieve alignment.

7.3 "Alignment" means aligning the expiry dates of certificates, SMC, ISSC and MLC.

7.4 "Aligned audits/inspection" means ISM and ISPS audits as well as MLC inspection conducted in conjunction with each other when a Company requests alignment.

7.5 "Adjusted Certificate" is the certificate or certificates, either SMC and/or ISSC and/or MLC, which will have its expiration date adjusted so as to achieve alignment.

8 OPENING AND CLOSING MEETINGS

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

(i) introduce the auditor to the ship's 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 necessary resources, documentation and facilities are available,
(vi) confirm the time and date of the closing meeting and any interim meetings.

8.2 The auditor shall verify the implementation of the approved SSP and objective evidence demonstrating the effectiveness of the documented procedures. This verification is achieved via interviews, review of documents and examination of records of drills and training.

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

9 REPORTING PLAN APPROVALS AND SHIPBOARD AUDITS

9.1 In the case of an SSP approval, the Letter of Approval includes 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".

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

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.

10 RESPONSIBILITIES PERTAINING TO AUDITS

10.1 TASNEEF's responsibilities

TASNEEF is responsible for performing the audit and certification process in accordance with these Rules and relevant flag State requirements.

10.2 Responsibilities of the auditor

10.2.1 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) organising any special technical assistance required to verify compliance,

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

10.2.2 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.

Confidentiality of all security data/information held or collected in occasion of the security activities foreseen by these Rules shall be always ensured also towards third parties.

11 ACTION FOLLOWING PORT STATE CONTROL DETENTIONS

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

11.2 Any Failures shall be dealt with in accordance with the relevant requirements of item 13.

11.3 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.

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.

13 FAILURES AND CORRECTIVE ACTION FOLLOW-UP

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

13.2 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.

13.3 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.

13.4 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.

13.5 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 to avoid recurrence. Additional audits may be carried out as necessary.

13.6 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 downgraded. 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.

13.7 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.

14 EMPLOYMENT OF ARMED GUARDS AND INSTALLATION OF CITADELS ON BOARD SHIPS THREATENED BY PIRACY IN THE INDIAN OCEAN

14.1 Companies duties

It is for the Company to decide what security measures should be adopted on board its ships based on the results of the ship security assessments. If, after assessing the risks to which a ship is exposed and after identifying its vulnerabilities, it is decided that armed guards or citadels have a part to play in the mix of deterrents and responses, then that is a matter for the Company's managers.
IMO Guidelines prohibit a Recognised Security Organisation (RSO) from approving, certifying or verifying processes and procedures that it has wholly or partially developed. A society and its auditors should not become involved in the detailed assessment of security risks or the selection of specific measures in relation to ships on which the society acts as an RSO. They should have no involvement in a Company's decisions as to whether armed guards should be employed or whether a citadel should be constructed, just as they should not be involved in other security-related decisions such as which areas must be restricted, how many CCTV cameras should be installed, where the SSAS activation points should be located or when to carry out additional deck patrols. No advice should be offered by RSOs and their auditors in relation to specific procedures and operations and no opinions should be expressed concerning the effectiveness or desirability of armed guards or whether citadels should be constructed in general.

14.2 Auditors duties

The RSO's role is to verify during approval stage of SSP and subsequent revision and during ISSC audits on board, that such decisions taken by the Company arise genuinely and rationally from the ship security assessment and that appropriate controls have been established and effectively implemented. For example, in relation to armed guards, auditors should verify that:

(i) the Company has taken steps to satisfy itself that the contractor is fit to provide the service,
(ii) the Company has taken steps to satisfy itself that the guards employed are adequately trained, qualified and experienced,
(iii) the Company has taken steps to ensure that the presence of armed guards and the corresponding procedures do not contravene any flag state requirements,
(iv) the Company has established procedures for ensuring that the measures adopted do not contravene the laws of States at whose ports the ship may call or through whose territorial waters it may pass,
(v) adequate procedures are in place to control the storage and deployment of weapons,
(vi) procedures governing the planning, coordination and execution of actions of the armed guards and of the crew in response to a security threat have been developed,
(vii) those involved understand what is required of them in the different threat scenarios,
(viii) all reasonably anticipated threat scenarios have been exercised and that any lessons learned have been applied to the response plans.

In accordance with item 5.4 of PR 24, auditors should verify that Companies have taken into account the guidance contained in the last revision of following IMO circulars:
MSC.1/Circ.1405 Rev.2 *"Revised Interim Guidance to Shipowners, Ship Operators, and Shipmasters on the use of Privately Contracted Armed Security Personnel on Board Ships in the High-risk Area".*
MSC.1/Circ.1406 Rev.3 *"Revised Interim Recommendations for Flag States Regarding the Use of Privately Contracted Armed Security Personnel on Board Ships in the High-risk Area".*
MSC.1/Circ.1443 *"Interim Guidance to Private Maritime Security Companies Providing Privately Contracted Armed Security Personnel On Board Ships in the High Risk Area"*
MSC-FAL.1/Circ.2*, Questionnaire on Information on Port and Coastal State Requirements Related to Privately Contracted Armed Security Personnel on board Ships*
MSC.1/Circ.1601/Rev.2 *"Revised Industry Counter Piarcy Guidance"*
In particular, Paragraph 5 of the Annex to MSC.1/ Circ.1406 states:
"Flag States should have in place a policy on whether or not the use of PCASP (privately contracted armed security personnel) will be authorised and, if so, under which conditions".
Furthermore, paragraph 3.1 of the Annex to MSC.1/Circ.1405 states:
"Ship owners should ensure that the Flag State is consulted at an early stage in their consideration of the decision to place PCASP on board to ensure that any statutory requirements are met".
In view of these recommendations, auditors should expect the Company to have consulted the Administration on its applicable requirements and policy and to have taken the necessary steps to ensure that applicable laws and guidelines are observed.

The Company should also have taken into account the best management practices contained in MSC.1/Circ.1339 *"Best Management Practices to Deter Piracy and Armed Robbery off the Coast of Somalia"* and be aware of the contents of MSC.1/Circ.1408 rev. 1 which contains guidance for port and coastal states.
As with any other IMO guidance, if a Company has chosen not to follow the advice in certain respects, it must be able to show that it has good reasons for doing so and that it has implemented measures that it believes will provide an equivalent level of control.

14.3 AUDITORS DUTIES WHEN CITADELS ARE INSTALLED ON BOARD

Where citadels are concerned, auditors should verify, for example, that:
- industry guidance, especially the latest version of industry best management practices, has been taken into account,
- guidance provided by the Maritime Security Centre – Horn of Africa (MSCHOA) and the NATO Shipping Centre has been taken into account,
- the Company has taken steps to ensure that any modifications to the ship or its equipment do not contravene class and statutory requirements or are the subjects of appropriate exemptions,
- adequate procedures are in place governing the activation, occupation and evacuation of the citadel,
- measures are in place to provide sufficient food and water,
- measures are in place so that adequate ventilation is provided and communications and system controls are established,
- appropriate exercises have been carried out.

This Guidance relates to the role and responsibilities of the classification societies when acting as RSOs for flag States. However it does not prevent them from offering, in their capacity as classification societies, technical support to a Company on associated issues relating to the maintenance of the vessel's class, provided that such support does not amount to advice on which measures to adopt, involvement in the development of specific operations and procedures or the expression of opinions concerning the usefulness and effectiveness of employing armed guards or constructing citadels.
Any such services provided in addition to the delegated audit and certification activities must not give rise to conflicts with a society's role as a RSO.

Annex 1 – MINIMUM REQUIREMENTS FOR ISPS CODE CERTIFICATION SCENARIOS

	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 subject to verification of compliance with QSCS in accordance with Section 5 of Annex 1 to the ~~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.
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.