Version	Date	Modification date	Editor
1.0	15.6.2026		Jan-Christian Welander

Guidance to Recognized Security Organizations (RSOs) on Ship Verification and Certification

Contents

1 Purpose and scope

This guidance is intended for RSOs authorized by Traficom to carry out ship security verification and certification activities under SOLAS chapter XI-2, the ISPS Code and Regulation (EC) No 725/2004.

2 Relationship with Traficom RO Agreement

This Guidance shall be read together with the Agreement Governing the Delegation of Statutory Certification Services for Ships Registered in Finland between Traficom and the RO, including Appendix 1, Degree of Authorization, and Appendix 2, Exchange of Information. For the purposes of

delegated ISPS functions, references to the RO include the Recognised Security Organisation (RSO), where applicable.

The RSO shall act only within the scope of authority formally delegated by Traficom.

Where this interim Guidance and the RO Agreement or its Appendices address the same subject, the RO Agreement and its Appendices shall prevail.

3 Mandatory Part B requirements under Regulation (EC) No 725/2004 Article 3(5)

For ships, and companies falling within the scope of Regulation (EC) No 725/2004, RSOs should treat the ISPS Code Part B paragraphs listed in Article 3(5) as mandatory EU requirements, not merely as guidance. Verification and certification procedures should therefore demonstrate how those mandatory Part B elements have been considered, sampled and recorded.

For ship verification and certification, the most directly relevant Article 3(5) requirements include: confidentiality of security plans and assessments; RSO recognition, competencies and independence; security level communication and implementation; identification documents; manning level; information to be supplied by the Company to the master; minimum standards for Ship Security Assessments and Ship Security Plans; revision of Ship Security Plans; and the frequency of ship security drills and exercises.

The RSO should verify that its own procedures and the ship's verification evidence address the mandatory Part B requirements that are relevant to the scope of the verification.

4 Authority and limits of RSO activity

The RO approving the Ship Security Plan shall not have been involved in the ship security assessment or in the preparation of the Ship Security Plan.
The ISPS audit shall be performed in the language stated in the Ship Security Plan.
The RSO shall ensure that its personnel, procedures and records demonstrate compliance with the applicable Traficom authorization, Regulation (EC) No 725/2004, SOLAS chapter XI-2, the ISPS Code, and the mandatory EU treatment of the relevant ISPS Code Part B provisions.
RSOs internal procedures should explicitly map Regulation (EC) No 725/2004, Article 3(5) mandatory ISPS Code Part B requirements to the relevant RSO activity, including RSO competence, independence, confidentiality, verification planning, findings and certification controls.

5 Types of ship verification

Interim verification: before an Interim International Ship Security Certificate (Interim ISSC) is issued, in the circumstances allowed by ISPS Code Part A section 19.4.1, to verify the prerequisites for interim certification under ISPS Code Part A section 19.4.2. This includes confirming that the Ship Security Assessment has been completed, the Ship Security Plan is on board, submitted for approval and being implemented, required security equipment including the Ship Security Alert System is provided, and arrangements are in place for drills, exercises, internal audits and the full verification within six months.

Initial verification: before the ship enters service or before the International Ship Security Certificate (ISSC) is issued for the first time. This must be a complete verification of the ship security system and any associated security equipment against SOLAS chapter XI-2, ISPS Code Part A, and the approved Ship Security Plan.

Intermediate verification: at least once during the certificate cycle. If only one intermediate verification is carried out, it must take place between the second and third anniversary date of the certificate and must be endorsed on the certificate. Where amendments have been made to an approved Ship Security Plan, the RSO should verify approval and implementation of every amendment since the previous verification or since the Ship Security Plan was originally approved.

Renewal verification: at intervals not exceeding five years, to confirm continued compliance and satisfactory condition of the ship security system and associated equipment.

Additional verification: additional verification may be required by Traficom, including where a ship returns to service after lay-up, after a security-related detention or where serious security-related concerns arise.

6 Pre-verification preparation

Confirm that the ship is within the scope of the RSO's authorization and delegation from Traficom.

Do not certify the ship under Finnish flag based on activities previously carried out on behalf of another flag State.

Confirm that the approved Ship Security Plan and related Ship Security Assessment address the minimum standards made mandatory through Article 3(5), including ISPS Code Part B paragraphs 8.3 to 8.10 and 9.2.

For Finnish-flag newbuildings, the RSO shall confirm whether the initial project meeting required by Traficom has been held or arranged between Traficom, the shipowner, the RO/RSO and the shipyard, where applicable.
For flag entry, the RSO shall confirm that Traficom, the RO/RSO and the shipowner have clarified the tasks and responsibilities for the transfer process, including any meeting considered necessary by Traficom.
The RSO shall verify that the intended ISPS activity is within the scope of the current Traficom authorization before carrying out the activity or issuing, endorsing or approving any security document on behalf of Traficom.

7 Conduct of onboard verification

The RSO auditor should verify implementation, not only documentation. The verification should confirm that the ship security system, associated equipment and the approved Ship Security Plan fully comply with SOLAS chapter XI-2, ISPS Code Part A and Part B made mandatory Regulation (EC) No 725/2004 Article 3(5).

Confirm that the approved Ship Security Plan is on board, protected from unauthorized access or disclosure, and implemented.

Review security records required under ISPS Code Part A section 10.

Confirm that the Ship Security Officer is designated, trained, familiar with the Ship Security Plan, and able to perform assigned responsibilities.

Confirm that observations and non-conformities from previous verifications have been addressed.

Confirm that the Company has provided the master with the information required by ISPS Code Part B paragraph 6.1, made mandatory by Article 3(5), concerning those responsible for appointing shipboard personnel and deciding employment of the ship.

Verify access control measures, restricted areas, cargo handling, delivery of ship's stores, handling of unaccompanied baggage, monitoring arrangements, communications, and response to security levels 1, 2 and 3, as addressed in the approved Ship Security Plan.

Verify that shipboard personnel with security duties understand their responsibilities and can perform assigned duties.

Verify that training, drills and exercises have been carried out and properly reported.

Verify drill and exercise frequency against ISPS Code Part B paragraphs 13.6 and 13.7 as mandatory requirements: drills at least every three months, a drill within one week where more than 25% of ship personnel have changed and have not participated in a drill on that ship within the previous

three months, and exercises at least once each calendar year with no more than 18 months between exercises.

Verify that security equipment, including the Ship Security Alert System is maintained, tested and recorded.

The RSO shall retain sufficient evidence to demonstrate that mandatory ISPS Code Part B requirements made mandatory under Regulation (EC) No 725/2004 Article 3(5) have been considered, sampled and recorded.

8 Findings, non-conformities and certification actions

Findings should be based on objective evidence, reported clearly and concisely, and explained to the Ship Security Officer and Master after completion of the verification.

A failure to implement a requirement made mandatory by Article 3(5) of Regulation (EC) No 725/2004 should be recorded as a non-compliance with the applicable EU maritime security requirements.

Where non-conformities prevent confirmation of full compliance, the RSO should not issue or endorse the ISSC until the non-conformity has been rectified and compliance has been verified.
The RSO shall inform Traficom without delay if the non-conformities are not rectified and the ISSC cannot be issued or endorsed.

9 Interim ISSC

An Interim ISSC may be issued only in the circumstances allowed by ISPS Code Part A section 19.4.1, including delivery, entry or re-entry into service, transfer of flag, or change of Company.

Before issuing an Interim ISSC, the RSO must verify that the Ship Security Assessment has been completed.

A copy of the Ship Security Plan meeting SOLAS chapter XI-2, ISPS Code Part A requirements and Regulation (EC) No 725/2004, Article 3(5) mandatory ISPS Code Part B requirements must be on board, submitted for review and approval, and being implemented.

10 Confidentiality and handling of security-sensitive information

RSOs must protect security-sensitive material from unauthorized access or disclosure. This includes Ship Security Assessments, Ship Security Plans, related approval records, verification records, and any information concerning vulnerabilities or security arrangements.

Under Regulation (EC) No 725/2004 Article 3(5), ISPS Code Part B paragraph 4.1 on protection of the confidentiality of security plans and assessments is mandatory in the EU context. RSOs should therefore ensure that access, storage, transmission and disposal arrangements for Ship Security Assessments, Ship Security Plans and related records prevent unauthorized disclosure.

11 Reporting and Exchange of information to Traficom

Submit verification and certification reports to Traficom in the format and within timeframe required by the RO Agreement (Appendix 2) and authorization terms.

Reports should record how Regulation (EC) No 725/2004, Article 3(5) mandatory Part B requirements were verified.

Approved Ship Security Plans, including the letter of approval, shall be sent to Traficom by secure e-mail or by another secure method required by Traficom.
Verification reports shall be made available to Traficom in accordance with the RO Agreement and Appendix 2, section 3.

12 Minimum RSO quality controls

Maintain documented procedures for auditor qualification, training, vetting and impartiality.

Maintain procedures for protection of security-sensitive information.

Maintain procedures for verification planning and conduct, use of objective evidence, classification and reporting of findings, certificate issue, endorsement and control, communication with Traficom, handling of urgent security-related failures, and retention and availability of verification and certification files.

Maintain a competence matrix for personnel performing security assessment, plan approval, verification and certification activities, reflecting the RSO competency expectations made mandatory through Article 3(5) and ISPS Code Part B paragraph 4.5.

Maintain impartiality controls to ensure that an RSO does not approve a Ship Security Plan or amendments for a ship where it prepared the Ship Security Assessment or Ship Security Plan, consistent with the independence requirement made mandatory through Article 3(5) and ISPS Code Part B paragraph 9.4.

13 Practical verification checklist for RSOs

13.1 Before verification

- Confirm ship, Company and certificate status.
- Confirm Ship Security Plan approval status and latest approved amendments.
- Confirm applicability of Regulation (EC) No 725/2004 and identify Article 3(5) mandatory Part B provisions relevant to the ship and verification type.
- Review previous verification findings, internal audits and corrective actions.
- Confirm whether interim, initial, renewal, intermediate or additional verification is required.

13.2 During verification

- Verify implementation of the approved Ship Security Plan.
- Verify access control, restricted areas, cargo, stores, baggage, monitoring and communications procedures.
- Verify SSO competence and crew familiarity.
- Verify training, drills, exercises and security records.
- Verify Ship Security Alert System and other security equipment maintenance, testing and records.
- Verify implementation of approved Ship Security Plan amendments.
- Verify that Article 3(5) mandatory Part B requirements are implemented where applicable
- Check that non-conformities are corrected or subject to appropriate corrective action before certification decisions.

13.3 After verification

- Explain deficiencies (if any) to the SSO and Master.
- Prepare an objective evidence-based report.
- Record Article 3(5) mandatory Part B requirements sampled and any related findings.
- Issue or endorse certificate only when compliance is confirmed.
- Report required information to Traficom.
- Protect all security-sensitive records.

14 Annex: Regulation (EC) No 725/2004 Article 3(5) mandatory ISPS Code Part B paragraphs

Article 3(5) of Regulation (EC) No 725/2004 requires Member States to conform to the following ISPS Code Part B paragraphs as if they were mandatory. RSOs should use this list as a cross-check when carrying out activities within the scope delegated by Traficom.

- 1.12 — revision of Ship Security Plans.
- 1.16 — Port Facility Security Assessment.
- 4.1 — protection of the confidentiality of security plans and assessments.
- 4.4 and 4.5 — Recognized Security Organizations and their minimum competencies.
- 4.8 — setting the security level.
- 4.14, 4.15 and 4.16 — contact points and information on Port Facility Security Plans.
- 4.18 — identification documents.
- 4.24 — ships' application of security measures recommended by the State in whose territorial waters they are sailing.
- 4.28 — manning level.
- 4.41 — communication of information when entry into port is denied or the ship is expelled from port.
- 4.45 — ships from a State which is not party to SOLAS.
- 6.1 — Company obligation to provide the master with information on the ship's operators.
- 8.3 to 8.10 — minimum standards for the Ship Security Assessment.
- 9.2 — minimum standards for the Ship Security Plan.
- 9.4 — independence of Recognized Security Organizations.
- 13.6 and 13.7 — frequency of security drills and exercises for ship crews, Company Security Officers and Ship Security Officers.

15 Sources

International Ship and Port Facility Security (ISPS) Code, Part A and Part B.

SOLAS chapter XI-2, Special measures to enhance maritime security.

Regulation (EC) No 725/2004 on enhancing ship and port facility security, including Article 3(5) and Annex III / ISPS Code Part B.

IMO MSC/Circ.1111, Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code.

IMO MSC/Circ.1132, Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code.

IMO Resolution MSC.159(78), Interim guidance on control and compliance measures to enhance maritime security.

Agreement governing the delegation of statutory certification services for ships registered in Finland between the Finnish Transport and Communications Agency (Traficom) and RO

Appendix 1, Degree of Authorization

Appendix 1, Degree of Authorization

Authorization of Recognized Security Organization (Decision)

EU MARSEC Handbook, Version 2024.