INSPENET

ISPS Compliance Audit Guide/Procedure ISPS (PBIP)

Date: 10/07/2025
Author: Mario Toyo, Engineer
Confidentiality: Internal Use Only

Contents

1. Introduction

This procedure/guide establishes the guidelines, criteria, and tools necessary to carry out ISPS Code compliance audits in port facilities. Its purpose is to verify the

degree of implementation of the required security measures, issue findings, and recommend whether or not to issue the Certificate of Compliance.

Scope: Applies to all port facilities that receive ships subject to the SOLAS Convention, including passenger ships and cargo ships with a gross tonnage of 500 GT or more.

Regulatory basis: SOLAS Convention 1974 (Chapter XI-2), ISPS Code, and current national regulations.

2. Assessment criteria

Organization and responsibilities

- Formal appointment of the FSO (facility security officer) and their deputy.
- Valid FSO certification in accordance with IMO standards.
- Authority and documented support from the designated authority.

Protection assessment (EPAF)

- EPAF valid for less than 5 years.
- Updated after incidents or significant changes.
- Incorporation of modern threats (cybersecurity, drones, internal sabotage).

Security plan (PPIP)

- Plan approved by the designated authority.
- Protocols for security levels 1, 2, and 3.
- Integration with emergency plans (fires, spills, evacuation).

Access control

- Credential systems, biometrics, or verifiable lists.
- Records of entry and exit of personnel, visitors, and vehicles.
- Video surveillance with a minimum retention period of 30 days.

Restricted areas

- Updated map and adequate signage.
- Access protocols with keys, cards, or biometrics.
- Record of entries and exits to these areas.

Training and exercises

- Annual staff training with documented records.
- Quarterly protection exercises.

- Annual drill in conjunction with external authorities and ships.

Certification and audits

- Current ISPS Certificate of Compliance (valid for 5 years).
- Internal audits with identification of non-conformities.
- Evidence of external audits.

Emergency integration

- Plans coordinated with fire, police, customs, and maritime authorities.
- Established emergency communication procedures.
- Inter-agency drills.

3. Verification Checklist

This checklist must be completed during the on-site audit.

1. Designated and Certified OPIP

Verification Question	Yes	No	Partial	Remarks
Is there a formal appointment of the OPIP?	☐	☐	☐	
Do the OPIP and the alternate hold valid certification?	☐	☐	☐	
Is the official resolution that accredits it available?	☐	☐	☐	

2. Updated PFSA (less than 5 years old)

Verification Question	Yes	No	Partial	Remarks
Is the PFSA less than 5 years old?	☐	☐	☐	
Does it include modern threats (cybersecurity, drones)?	☐	☐	☐	
Was it updated after relevant incidents?	☐	☐	☐	

3. Security plan approved by the authority

Verification Question	Yes	No	Partial	Remarks
Is the PFSP approved by the Designated Authority?	☐	☐	☐	

Verification Question	Yes	No	Partial	Remarks
Does it include protocols for levels 1, 2, and 3?	☐	☐	☐	
Has it been disseminated among key personnel?	☐	☐	☐	

4. Access control with auditable records.

Verification Question	Yes	No	Partial	Remarks
Are there entry and exit records available?	☐	☐	☐	
Is the access control system reliable and audited?	☐	☐		
Are surveillance cameras available with a minimum storage of 30 days?	☐	☐	☐	

5. Restricted areas signposted and controlled

Verification Question	Yes	No	Partial	Remarks
Are the areas properly signposted?	☐	☐	☐	
Is access controlled through security systems?	☐	☐	☐	
Are entries and exits in these areas recorded?	☐	☐	☐	

6. Annual staff training

Verification Question	Yes	No	Partial	Remarks
Has the staff received ISPS training within the last year?	☐	☐	☐	
Are there documented training records available?	☐	☐	☐	
Does the training include practical exercises?	☐	☐	☐	

7. Quarterly drills and annual exercise

Verification Question	Yes	No	Partial	Remarks
Have quarterly drills been conducted?	☐	☐	☐	
Has an annual joint exercise been carried out with external authorities?	☐	☐	☐	
Have minutes or reports been prepared for each exercise?	☐	☐	☐	

8. Current ISPS compliance certificate

Verification Question	Yes	No	Partial	Remarks
Does the port have a current compliance certificate?	☐	☐	☐	
Is the validity date current and correct?	☐	☐	☐	
Is the certificate displayed or available on site?	☐	☐	☐	

9. Measures Defined for Levels 1, 2 and 3

Verification Question	Yes	No	Partial	Remarks
Are there differentiated protocols for each level?	☐	☐	☐	
Does the staff know the specific measures?	☐	☐	☐	
Have practical exercises been conducted for levels 2 and 3?	☐	☐	☐	

10. Integration with Emergency Plans

Verification Question	Yes	No	Partial	Remarks
Is the Security Plan integrated with other emergency plans?	☐	☐	☐	
Have joint exercises been coordinated?	☐	☐	☐	

Verification Question	Yes	No	Partial	Remarks
Is there an established communication channel for emergencies?	☐	☐	☐	

4. Final audit report template

1. General Information

Port Facility Name: _____
Location: _____
Port Authority / Concessionaire: _____
Audit Date: ____/____/_____
Lead Auditor: _____
Audit Team: _____
ISPS Officer / Alternate: _____
Protection Level in force during the audit: _____

2. Executive summary

This section provides a summary of the main findings of the audit, including the observed level of compliance, strengths, and areas requiring improvement. This summary will serve as the basis for the recommendation regarding the issuance or non-issuance of the ISPS Compliance Certificate.

3. Audit results

Audited Area	Non-Conformities (NC)	Observations (OBS)	Best Practices (BP)
Organization and Responsibilities			
Protection Assessment (PFSA)			
Security Plan (PPIP)			
Access Control			
Restricted Areas			
Training and Exercises			

Audited Area	Non-Conformities (NC)	Observations (OBS)	Best Practices (BP)
Certification and Audits			
Integration with Emergencies			

4. Classification of findings

- NC (Non-Conformity): Direct non-compliance with the ISPS Code that may prevent certification.
- OBS (Observation): Weakness detected that does not break compliance but requires improvement.
- BP (Best Practice): Outstanding practice that exceeds the requirements of the Code.

5. Auditor's recommendation

Based on the findings, the auditor recommends the following:

□ Issue / renew the ISPS Compliance Certificate.
□ Issue conditionally upon correction of minor NCs within ____ days.
□ Do not issue until the critical NCs detected are remedied.

5. Signatures

Lead Auditor: _____ Date: : ____/____/_____
ISPS Officer / Port Representative: _____ Date: : ____/____/_____