

Maritime Security Management and ISPS Compliance Training Course

21 – 25 December 2026
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Maritime Security Management and ISPS Compliance Training Course

Ref: 2143_256922 **Date:** 21 – 25 December 2026 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Maritime Security Management and ISPS Code Compliance Training Course is a one-week intermediate course for ship, company, and port facility security personnel and maritime managers, who leave with a Maritime Security and ISPS Compliance Assurance Plan. Participants apply maritime security risk assessment, security levels, plans, records, drills, audits, incident coordination, and corrective action across ship-port interfaces. Agile Leaders Training Center presents maritime security management and ISPS Code compliance.

Who Should Attend

- Personnel responsible for ship, company, or port facility security arrangements
- Maritime managers responsible for compliance, operations, and assurance
- Port personnel responsible for access control, restricted areas, and security records
- Audit and quality personnel responsible for testing security-plan effectiveness
- Emergency and liaison teams responsible for ship-port incident coordination

The course assumes participants can interpret maritime procedures and operational risk information, and it leaves role certification, weapons handling, and jurisdiction-specific enforcement outside its scope.

Departments and Industries

The course supports departments and sectors that manage security across international shipping and port operations.

- Shipping companies and vessel operations
- Ports, terminals, and port facility management
- Maritime transport, logistics, and cargo handling
- Offshore, energy, and marine service operations
- Security assurance, audit, and emergency coordination functions

Learning Objectives

By the end of this course, participants will be able to:

- Apply SOLAS chapter XI-2 and ISPS Code responsibilities.
- Analyze threats, vulnerabilities, and security-level implications.
- Build ship-port security controls, plans, and records.
- Evaluate drills, audits, incidents, and corrective actions.
- Prioritize coordination, communication, and information protection.
- Build a Maritime Security and ISPS Compliance Assurance Plan.

Course Agenda

Day 1: Map the ISPS Security Framework

- SOLAS Chapter XI-2 and ISPS Code Structure Map
- Part A Requirement and Part B Guidance Matrix
- Contracting Government, Company, Ship, and Port Responsibility Chart
- Company, Ship, and Port Facility Security Officer Interface Map
- Maritime Security Information and Confidentiality Control Checklist

Day 2: Assess Threats and Set Controls

- Ship and Port Facility Security Assessment Method
- Threat, Asset, Vulnerability, and Consequence Register
- Security Level 1, 2, and 3 Control Decision Matrix
- Access, Restricted Area, Cargo, Stores, and Monitoring Control Map
- Proportionate Maritime Security Measure Selection Tool

Day 3: Manage Plans and Ship-Port Interfaces

- Ship Security Plan and Port Facility Security Plan Crosswalk
- Declaration of Security Trigger and Responsibility Checklist
- Communication, Alert, Reporting, and Escalation Protocol
- Visitor, Contractor, Crew, and Shore-Leave Access Control Plan
- Security Record, Retention, and Change-Control Register

Day 4: Assure Compliance and Response

- ISPS Compliance Audit and Evidence Sampling Plan
- Drill and Exercise Objective, Scenario, and Evaluation Matrix
- Security Incident Command and Ship-Port Coordination Map
- Nonconformity, Root-Cause, and Corrective-Action Log
- Management Review and Continual Improvement Dashboard

Day 5: Practice Maritime Security Assurance

- Suggested Exercise: Map ISPS Roles and Security Information
- Suggested Exercise: Assess a Ship-Port Threat Scenario
- Suggested Exercise: Build a Declaration of Security Decision
- Suggested Exercise: Evaluate a Drill and Corrective Action
- Capstone Exercise: Complete a Maritime Security and ISPS Compliance Assurance Plan

Practical Exercises

The course uses suggested activities based on vessel, terminal, cargo, access, and incident scenarios.

- Suggested activity: assign ISPS responsibilities and information flows across company, ship, port facility, and authority interfaces.
- Suggested activity: assess threats and vulnerabilities, determine security-level implications, and select proportionate controls.
- Suggested activity: review plan alignment, Declaration of Security triggers, access arrangements, and protected records.
- Suggested activity: evaluate a drill, identify assurance evidence, analyze causes, and define corrective actions.

FAQs

Who suits maritime security management and ISPS Code compliance training, and what does it assume?

Maritime security management and ISPS Code compliance training suits security personnel, maritime managers, port teams, auditors, and incident coordinators. It assumes experience interpreting maritime procedures and operational risks.

How does ISPS Code compliance training differ from Ship Security Officer training?

ISPS Code compliance training integrates management, ship-port interfaces, assurance, audits, drills, incidents, and improvement. Ship Security Officer training focuses on the designated role and its defined duties.

How do ISPS security levels affect maritime security measures?

ISPS security levels determine the intensity of protective measures. Ships and port facilities align access, monitoring, cargo, communication, and response arrangements with the level communicated by the responsible authority.

AGILE LEADERS
Training Center

When is a Declaration of Security used under the ISPS framework?

A Declaration of Security records agreed responsibilities between a ship and port facility, or between ships, when circumstances require explicit coordination of security measures.

How should ISPS drills and audits support compliance assurance?

ISPS drills and audits should test objectives, responsibilities, communications, records, control performance, and response coordination, then turn findings into documented corrective actions and management review.

Conclusion

Participants take back a Maritime Security and ISPS Compliance Assurance Plan. It combines responsibilities, risk assessment, security levels, controls, plans, ship-port coordination, records, drills, audits, incidents, and corrective action. The plan changes separate security activities into a traceable management system for proportionate maritime protection and continual improvement.