JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Maritime Security Management to the ISPS Code Course

24 January – 4 February 2027
Dubai

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Maritime Security Management to the ISPS Code Course

Ref: 486_17805 **Date:** 24 January – 4 February 2027 **Location:** Dubai **Fees:** 8000 GBP

Maritime Security Management to the ISPS Code is an advanced 2-week training course for port facility security officers, company security officers and ship security officers who keep assessments, plans and drills effective, ending with a Security Plan Review for a port facility or ship. Piracy, stowaways, smuggling and attacks on terminals keep shifting, while ship and shore interfaces grow busier. Jupiter Prime Training delivers this course to officers already holding security duties.

Why Maritime Security Management to the ISPS Code Matters Now

Three pressures shape maritime security today: threats that move between sea lanes, anchorages and terminals faster than plans are revised, inspections that test whether measures work in practice, and commercial partners who expect ship and port to coordinate without delaying cargo. A facility or fleet that manages security well keeps trading at higher security levels with little disruption, while one that manages it badly faces detentions, delays and exposed crews. The course rests on the International Ship and Port Facility Security ISPS Code of the International Maritime Organization IMO and draws on IMO model courses for security officers.

Who Gains Most from Maritime Security Management to the ISPS Code

- Port facility security officers who keep the facility assessment and plan current
- Company security officers who oversee ship security across a fleet and liaise ashore
- Ship security officers who run onboard measures, searches and drills
- Terminal operations leads who balance cargo flow against access and screening controls
- Marine superintendents who approve security budgets and crew preparation

A shipping company and the terminal operator it calls at gain most when their company, ship and port facility security officers attend together, because they can agree declarations of security, communication routes and drill scenarios across the ship and shore interface.

Maritime Security Management to the ISPS Code Capabilities

Participants move from holding the plan on file to proving and exercising it against current threats.

- Assess ship and port facility vulnerabilities through structured assessments — officers prioritising plan amendments
- Design measures for each security level covering access, restricted areas and cargo handling — masters and terminal managers
- Specify search, screening and stowaway prevention routines — gangway and gate teams applying them consistently
- Test plans through drills and exercises with measurable objectives — company and facility officers judging readiness
- Build declaration of security and ship and shore communication arrangements — vessels and terminals sharing duties
- Communicate incident reports to owners, charterers and port authorities — fleet and facility decisions

Key Maritime Security Management to the ISPS Code Terms

- ISPS Code — the international framework setting security duties for ships, shipping companies and port facilities.
- Port facility security assessment PFSA — a structured evaluation of a facility's assets, threats and weaknesses that underpins its plan.
- Ship security plan SSP — the document setting out the measures a ship applies at each security level, including access and restricted areas.
- Security level — one of three graded states setting how strict ship and facility measures must be.
- Declaration of security DoS — an agreement between a ship and a facility or another ship stating who carries out each measure.
- Restricted area — a zone on a ship or in a facility where access is limited to authorised persons for protection of sensitive spaces.

Maritime Security Management to the ISPS Code Day by Day

Day 1: The Maritime Threat Picture

- Maritime Threat Typologies — Comparing Piracy, Armed Robbery, Smuggling and Sabotage
- Stowaway and Unauthorised Boarding Patterns — Recognising Common Methods
- Threat Intelligence Sources for Shipping — Updating Voyage Risk Briefings
- Ship and Shore Interface Risks — Locating Gaps Between Vessel and Terminal
- Lessons From Maritime Security Incidents — Testing Current Assumptions

Day 2: The ISPS Code Framework

- ISPS Code Structure and Parts — Separating Mandatory Duties From Guidance
- Roles of Company, Ship and Port Facility Security Officers — Allocating Responsibilities
- Security Levels One to Three — Setting Triggers and Escalation
- Records and Documentation Requirements — Preparing for Inspections
- IMO Model Course Content — Benchmarking Officer Competence

Day 3: Port Facility Security Assessment

- PFSA Methodology — Identifying Assets, Infrastructure and Critical Operations
- Threat Scenario Selection for Terminals — Choosing Credible Attack Paths
- Vulnerability Scoring of Berths and Gates — Ranking Weak Points
- Waterside and Landside Approaches — Assessing Perimeter Exposure
- Assessment Report Writing — Supporting Plan Amendments

Day 4: Ship Security Assessment

- On-Scene Security Survey — Walking the Vessel Deck by Deck
- Restricted Area Designation Onboard — Protecting Bridge, Engine Room and Stores
- Trading Pattern Risk Review — Matching Routes to Threat Levels
- Crew Vulnerability and Insider Risk — Screening Shipboard Access
- Ship Security Assessment Records — Feeding the Ship Security Plan

Day 5: Security Plans and Measures

- Port Facility Security Plan Structure — Linking Measures to Each Security Level
- Ship Security Plan Content — Setting Access, Handling and Monitoring Duties
- Access Control at Gangways and Gates — Verifying Identity and Purpose
- Cargo, Stores and Baggage Screening — Detecting Prohibited Items
- Plan Amendment Control — Keeping Approved Versions Current

Day 6: Ship and Shore Coordination

- Declaration of Security Procedures — Dividing Duties Between Ship and Facility
- Communication Plans and Alert Routes — Reaching Authorities Quickly
- Ship Security Alert Systems — Testing Covert Alarm Procedures
- Shore Leave and Crew Change Controls — Managing People at the Interface
- Contractor and Visitor Management at Terminals — Controlling Temporary Access

Day 7: Countering Specific Threats

- Best Management Practices Against Piracy — Hardening Vessels in Risk Areas
- Stowaway Search Routines — Clearing Holds, Containers and Voids
- Smuggling Detection Indicators — Spotting Concealment in Cargo and Stores
- Underwater and Small Craft Threats — Protecting Hulls and Moorings
- Citadel and Safe Muster Procedures — Protecting Crew During Attack

Day 8: Drills, Exercises and Training

- Drill Schedule Design — Covering Every Plan Element Over Time
- Tabletop and Live Exercise Scenarios — Testing Coordination Across Agencies
- Exercise Objectives and Evaluation Criteria — Measuring Performance
- Security Awareness for Personnel With Duties — Building Competence Onboard and Ashore
- Post-Exercise Reports — Turning Findings Into Plan Changes

Day 9: Audits, Incidents and Continual Improvement

- Internal Security Audits — Verifying Plan Implementation
- Security Incident Reporting — Recording Breaches and Suspicious Activity
- Incident Response and Evidence Preservation — Supporting Investigations
- Inspection Readiness Checklists — Preparing for Port and Flag Visits
- Corrective Action Tracking — Closing Audit and Drill Findings

Day 10: Practising the Security Plan Review

- Applying the PFSA or Ship Assessment — Confirming Threats for a Chosen Site
- Applying Security Level Measures — Testing Access and Screening Controls
- Applying Drill and Audit Findings — Prioritising Plan Amendments
- Applying Ship and Shore Coordination — Updating Declarations and Contacts
- Security Plan Review — Recording Gaps, Amendments and Owners

Applying Maritime Security Management to the ISPS Code After the Course

- Lead a structured review of the port facility or ship security assessment, updating threat scenarios and vulnerability scores with the operations lead.
- Run a security drill on stowaway search or access control with set objectives, and report findings and plan amendments to the company security officer.

Maritime Security Management to the ISPS Code Questions FAQ

What is maritime security management to the ISPS Code and why does it matter now?

Maritime security management to the ISPS Code is the work of assessing, planning, exercising and auditing security on ships and in port facilities. It matters now because threats shift quickly and inspections test whether measures work in practice.

Which roles gain most from maritime security management to the ISPS Code training?

Port facility, company and ship security officers gain most from maritime security management to the ISPS Code training.

How does maritime security management to the ISPS Code differ from a port operations course?

Maritime security management to the ISPS Code focuses on threats, assessments, security plans, drills and audits. A port operations course focuses on berth planning and cargo flow.

What do you bring back from maritime security management to the ISPS Code training?

You bring back a Security Plan Review for a port facility or ship. It records threats, gaps, drill findings and amendments with owners.

Maritime Security Management to the ISPS Code: The Way Forward

The Security Plan Review first informs which amendments a port facility or ship security plan needs before its next drill or inspection. Security officers, masters and terminal managers use it to coordinate measures across the ship and shore interface. After the next exercise, revisit the threat scenarios against what was observed, at a container terminal or a tanker berth alike, so the plan stays credible.