ISPS Code Implementation: Port Facility Security, PFSO Duties and Ship/Port Interface

15 – 19 February 2027
London - Central London four-star



ISPS Code Implementation: Port Facility Security, PFSO Duties and Ship/Port Interface

Ref: 180_10569 **Date:** 15 – 19 February 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

ISPS Code implementation breaks down at port facilities when the security assessment is out of date, the security plan sits on a shelf, gate staff cannot say what changes at a higher security level and nobody has drilled the response to a stowaway or a suspicious package. This Core Concept course gives port facility and terminal security staff a working method to apply the Code on the berth and at the ship/port interface, from assessment and plan through access control, screening, drills and records. Participants produce a Port Facility Security Plan Gap Review and Drill Programme for their own facility.

Course Objectives:

- Apply the mandatory Part A requirements and Part B guidance of the ISPS Code to the daily security routine of a port facility
- Carry out a port facility security assessment and turn its findings into port facility security plan measures for each security level
- Coordinate security duties between the port facility security officer, ship security officer and company security officer, including declarations of security
- Operate access control, restricted area, cargo and ship's stores screening procedures that change in step with security levels 1, 2 and 3
- Plan and evaluate security drills and exercises and respond to and report maritime security incidents such as stowaways, smuggling and suspicious items
- Maintain ISPS security records and run internal audits and reviews that keep the security plan current

Target Audience:

- Staff who hold or deputise for the port facility security officer duty at a terminal, berth or offshore loading facility
- Terminal security supervisors who run gates, patrols, screening points and restricted area controls
- Ship and fleet security staff who handle the ship security officer or company security officer duty at the ship/port interface
- Port operations and harbour staff who coordinate vessel calls, cargo and stores deliveries with security teams
- HSE and emergency response staff who integrate security incidents into facility emergency procedures
- Internal auditors and compliance staff who review security records and plan implementation at maritime facilities

Course Outline:

Day 1: ISPS Code Structure, SOLAS Chapter XI-2 and the Maritime Threat Picture

- SOLAS Chapter XI-2 Special Measures to Enhance Maritime Security and the Role of Contracting Governments
- ISPS Code Part A Mandatory Requirements Versus Part B Recommendatory Guidance
- Security Levels 1, 2 and 3: Setting, Communication and Response Expectations
- Maritime Threat Types: Piracy, Armed Robbery, Stowaways, Smuggling and Cyber Attacks at Overview
- Port Facility ISPS Current-State Self-Assessment Checklist

Day 2: Port Facility Security Assessment, Security Plan and Security Officer Roles

- Port Facility Security Assessment Method: Critical Assets, Threat Scenarios and Weakness Identification
- Port Facility Security Plan Structure: Measures per Security Level and Plan Protection
- Port Facility Security Officer Duties, Authority and Training Records
- Ship Security Officer and Company Security Officer Duties and the Ship Security Plan Link
- Ship Security Alert System, SUA Convention and LRIT Ship Tracking at Overview

Day 3: Ship/Port Interface, Access Control and Cargo and Stores Screening

- Declaration of Security: Triggers, Content and Sign-Off Between Ship and Port Facility
- Access Control at Gates and Quay: Identity Verification, Pass Systems and Seafarer Shore Leave
- Restricted Area Designation, Marking, Monitoring and Unauthorised Entry Response
- Cargo Handling Security: Seal Checks, Manifest Reconciliation and Container Screening
- Ship's Stores and Unaccompanied Baggage Screening and Delivery Control

Day 4: Security Drills, Exercises, Incident Response and Cyber Risk at the Port

- Security Drill and Exercise Programme: Frequency Planning, Scenarios and Debrief Records
- Stowaway Detection, Search Patterns and Handover Procedure at the Berth
- Suspicious Package, Bomb Threat and Unauthorised Vessel Approach Response Flow
- Maritime Security Incident Reporting Chain and Security Level Escalation
- Port and Ship Cyber Risk: Phishing, Ransomware and Operational System Exposure at Overview

Day 5: Port Facility Inspection Walkthrough and Security Plan Gap Review

- Guided Walkthrough: Gate, Perimeter and Restricted Area Control Scoring
- Guided Walkthrough: Berth, Cargo Screening and Ship's Stores Delivery Points
- ISPS Security Records Review and Internal Audit Sampling Exercise
- Tabletop Exercise: Security Level 2 Escalation With a Vessel Alongside
- Port Facility Security Plan Gap Review and Drill Programme Build and Peer Review

Skills You Will Gain:

- Port Facility Security Assessment
- Security Plan Maintenance
- Ship/Port Interface Coordination
- Security Level Response
- Access and Restricted Area Control
- Cargo and Stores Screening
- Security Drill Design
- Security Record Auditing

Why Attend This Course:

- Return with a Port Facility Security Plan Gap Review and Drill Programme prepared for your own facility
- Brief gate, patrol and screening staff on exactly what changes when the security level rises
- Handle a vessel call with a clear declaration of security and agreed contacts between ship and facility
- Compare ISPS practice with security peers from container, bulk, oil and gas, and passenger terminals

Conclusion:

Maritime and port facility security holds when the ISPS Code is lived at the gate, the quay and the ship/port interface, not only written in a plan. The course moves from the Code structure, SOLAS chapter XI-2 and threat types, through assessment, plan and officer roles, to declarations of security, access control and screening, then to drills, incident response and cyber risk. The final day applies it all in a facility walkthrough and produces a Port Facility Security Plan Gap Review and Drill Programme for the next review cycle.