



Security Awareness (ISPS Code/Site Security)

18 – 22 October 2026
Kuala Lumpur (Malaysia)



Security Awareness (ISPS Code/Site Security)

Ref: 16314_1015368 **Date:** 18 – 22 October 2026 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4600 Euro

Introduction:

Security in maritime and port operations has become a critical priority worldwide. The ISPS Code provides a structured framework for maintaining high-level security standards at ports, ships, and associated facilities. This Security Awareness ISPS Code/Site Security course equips participants with an understanding of security risks, threats, and mitigation strategies, aligning with international regulations and best practices. They will explore preventive measures, threat identification, and response protocols essential to safeguarding personnel, assets, and operations.

The Security Awareness ISPS Code/Site Security program emphasizes proactive security awareness and incident management to minimize potential disruptions. Real-life scenarios and practical exercises reinforce theoretical knowledge, ensuring effective learning outcomes. Professionals will gain the skills necessary to maintain compliance and implement robust security strategies in maritime environments.

Targeted Groups:

This Security Awareness ISPS Code/Site Security course targets professionals seeking specialized knowledge and skills:

- Port security officers seeking regulatory compliance expertise.
- Shipboard personnel responsible for onboard safety and security.
- Maritime operations managers oversee port and vessel activities.
- Facility security personnel ensure adherence to security plans.
- Auditors and inspectors are evaluating the implementation of the ISPS Code.
- Security consultants providing risk assessments in maritime contexts.
- Crew members involved in emergency response and evacuation procedures.
- Compliance officers responsible for policy enforcement.
- Logistics and supply chain managers handling sensitive cargo.
- Maritime training instructors seeking up-to-date security practices.

Targeted Competencies:

Participants will gain the following competencies during the Security Awareness ISPS Code/Site Security program:

- Practical knowledge of ISPS Code compliance.
- Risk identification and threat assessment skills.
- Proficiency in security plan development and implementation.
- Emergency response and incident management capabilities.
- Effective communication within security teams.
- Auditing and evaluating security measures accurately.
- Strategic planning for maritime and port security.
- Awareness of international maritime security standards.
- Problem-solving skills in complex operational scenarios.
- Enhanced ability to protect personnel, assets, and operations.

Course Objectives:

Participants will achieve the following objectives by completing the Security Awareness ISPS Code/Site Security course:

- Understand the ISPS Code structure and key requirements.
- Identify potential security threats to vessels and port facilities.
- Apply preventive measures to effectively mitigate risks.
- Develop security awareness programs tailored to meet the organization's specific needs and requirements.
- Evaluate the effectiveness of security protocols through audits.
- Implement emergency response plans in the event of security incidents.
- Enhance communication and coordination among security teams.
- Assess vulnerabilities in maritime operations and propose improvements.
- Analyze security documentation and compliance reports efficiently and effectively.
- Strengthen decision-making in real-time threat scenarios.
- Integrate international regulations into local security procedures.
- Promote a culture of security awareness among all personnel.
- Maintain accurate records and logs to ensure compliance with regulatory inspections and requirements.
- Enhance your risk assessment skills with practical examples.
- Adapt security strategies to evolving threats and technological changes.

Studying Scenarios:

In this Security Awareness ISPS Code/Site Security training, participants will develop their skills through the analysis of the following scenarios:

- Unauthorized access attempts to port facilities.
- Suspicious cargo handling and reporting procedures.
- Security breaches during vessel docking and undocking operations.
- Coordination between ship security and port authorities.
- Response to simulated onboard threats and intrusions.
- Implementation of emergency evacuation plans under pressure.
- Risk assessment of high-profile or sensitive cargo movements.
- Communication challenges during multi-agency security operations.
- Detecting insider threats within maritime personnel.
- Scenario-based audit of compliance documentation and reporting.

Course Content:

Unit 1: Introduction to Maritime Security & ISPS Code:

- Overview of international maritime security requirements.
- Objectives and scope of the ISPS Code.
- Key definitions and terminology in marine security.
- Roles and responsibilities of security personnel.
- Security levels and alert protocols.
- Regulatory authorities and compliance expectations.
- Historical case studies of marine security breaches.

Unit 2: Threats, Risks, and Vulnerabilities:

- Identifying external and internal security threats.
- Understanding Terrorist and Criminal Activities in Ports.
- Vulnerability assessment for vessels and facilities.
- Risk analysis techniques and prioritization.
- Threat detection methods using modern technology.
- Common maritime security pitfalls and mitigation strategies.
- Reporting and documenting identified risks.

Unit 3: Security Planning & Preventive Measures:

- Developing vessel and facility security plans.
- Access control procedures for personnel and cargo.
- Physical security measures and surveillance systems.
- Security patrols, monitoring, and reporting routines.
- Contingency planning and resource allocation.
- Security awareness training for all personnel.
- Integration of technology in preventive security measures.
- Coordination with law enforcement and emergency agencies.

Unit 4: Emergency Response & Incident Management:

- Incident reporting procedures and protocols.
- Response Strategies for Security Breaches and Threats.
- Evacuation and emergency drills for port and vessel staff.
- Coordination between internal teams and external authorities.
- Handling suspicious packages and hazardous situations.
- Communication strategies during high-stress incidents.
- Post-incident analysis and lessons learned.

Unit 5: Compliance, Auditing & Continuous Improvement:

- Conducting security audits for vessels and facilities.
- Documentation and record-keeping requirements.
- Evaluation of security plan effectiveness.
- Continuous monitoring and improvement strategies.
- Benchmarking against international standards.
- Integration of feedback into security operations.
- Training updates and refresher courses for personnel.
- Future Trends in Maritime Security and ISPS Compliance.

Final Insights & Key Takeaways:

Security awareness is a critical component of maritime operations. Effective implementation of the ISPS Code enhances protection for personnel, vessels, and port facilities. Continuous training, risk assessment, and proactive measures reduce potential threats. This course empowers participants to develop, implement, and evaluate robust security practices for sustained operational safety.