Maritime Risk and Port Security Basics Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The global maritime domain is the lynchpin of international commerce, with over 90% of world trade relying on shipping. This dependence creates an irresistible target for threats ranging from traditional piracy and smuggling to contemporary challenges like sophisticated cyber-attacks and acts of maritime terrorism. This escalating threat landscape necessitates a mandatory, standardized, and dynamic approach to security. The International Ship and Port Facility Security (ISPS) Code, implemented through the SOLAS Convention, forms the fundamental international governance framework for mitigating these risks.

Maritime Risk and Port Security Basics Training Course provides personnel with the foundational knowledge and practical skills required to effectively enhance security measures within their roles. By focusing on threat recognition, vulnerability assessment, and rigorous security plan implementation across all three mandatory Security Levels, participants will become the first line of defence. The curriculum uniquely blends established physical security protocols with an emphasis on emerging risks, particularly in Operational Technology (OT) systems and supply chain security, ensuring port facilities and vessels maintain operational continuity and regulatory compliance in an increasingly volatile and digitized environment.

Programme Curriculum

Maritime Risk and Port Security Basics Training Course

Introduction

The global maritime domain is the lynchpin of international commerce, with over 90% of world trade relying on shipping. This dependence creates an irresistible target for threats ranging from traditional piracy and smuggling to contemporary challenges like sophisticated cyber-attacks and acts of maritime terrorism. This escalating threat landscape necessitates a mandatory, standardized, and dynamic approach to security. The

International Ship and Port Facility Security (ISPS) Code, implemented through the SOLAS Convention, forms the fundamental international governance framework for mitigating these risks.

Maritime Risk and Port Security Basics Training Course provides personnel with the foundational knowledge and practical skills required to effectively enhance security measures within their roles. By focusing on threat recognition, vulnerability assessment, and rigorous security plan implementation across all three mandatory Security Levels, participants will become the first line of defence. The curriculum uniquely blends established physical security protocols with an emphasis on emerging risks, particularly in Operational Technology (OT) systems and supply chain security, ensuring port facilities and vessels maintain operational continuity and regulatory compliance in an increasingly volatile and digitized environment.

Course Duration

5 days

Course Objectives

Upon successful completion of this course, participants will be able to:

1. Define the principles of the ISPS Code and its mandatory application in a modern port environment.
2. Differentiate between the three international Security Levels and outline the specific security actions required for each.
3. Conduct basic Port Facility Security Assessments (PFSA) to identify physical and procedural vulnerabilities.
4. Implement and maintain effective Access Control measures for personnel, vehicles, and ship-port interfaces.
5. Recognise and report suspicious activities, focusing on signs of Insider Threat and unauthorized surveillance.
6. Understand fundamental concepts of Maritime Cyber Resilience to protect critical OT systems and data networks.
7. Detail security protocols for the secure handling and segregation of Cargo Integrity and ship's stores.
8. Participate effectively in Security Drills and Exercises for preparedness against security incidents.
9. Apply the procedures for completing a Declaration of Security (DoS) between ship and port.
10. Identify and respond to potential threats related to Narcotics Trafficking and the carriage of Weapons or dangerous substances.
11. Explain the role of Physical Security Equipment, including CCTV, barriers, and intrusion detection systems.
12. Contribute to maintaining Supply Chain Security by verifying documentation and monitoring intermodal transfers.
13. Communicate security-related information efficiently using established Security Communication Protocols.

Target Audience

1. Port Terminal Operations Staff
2. Port Facility Security Guards/Patrol Personnel
3. Vessel/Ship Crew
4. Contractors and Vendors with routine access to restricted port areas
5. Administrative and Clerical Staff working within the port facility
6. Customs and Border Protection Agents with port-related duties
7. Cargo Handlers and Stevedores responsible for loading/unloading

8. Government Agency Inspectors with facility oversight duties

Course Modules

Module 1: The ISPS Code and Maritime Security Framework

- The history and objectives of the SOLAS Convention and the ISPS Code
- Understanding the three Security Levels and corresponding response actions.
- Roles and responsibilities of key stakeholders.
- Introduction to the Port Facility Security Assessment and its importance in risk management.
- Case Study: Post-9/11 regulatory changes and the global rollout impact of the ISPS Code.

Module 2: Threat Identification and Recognition

- Identification of traditional threats: Piracy, Armed Robbery, Terrorism, Smuggling
- Understanding Insider Threat vectors and recognising suspicious behaviour/unauthorised surveillance.
- The risk of Stowaways and illegal migration and the search procedures required.
- Recognising Improvised Explosive Devices and basic bomb threat response.
- Case Study: The Mumbai Attacks (2008).

Module 3: Port Access Control Procedures

- Fundamentals of Access Control at the port perimeter and points of entry/exit.
- Procedures for checking and verifying Security Identification Documents and badges.
- Controlling access for Vehicles and methods of routine vehicle inspection.
- Managing access to Restricted Areas and the control of keys and electronic passes.
- Case Study: Port of Charleston Perimeter Breach.

Module 4: Cargo and Stores Security

- Procedures for maintaining Cargo Integrity and detecting tampering or suspicious cargo.
- Security measures for handling dangerous goods and hazardous materials.
- Supervision of Ship’s Stores and the security of delivery vehicles and personnel.
- Understanding the concept of the "Container Security Initiative" and seal checks.
- Case Study: Large-scale narcotics seizure via hull-fouling or container insertion

Module 5: Vessel and Ship/Port Interface Security

- Implementing the Declaration of Security and when it is required.
- Security requirements for the Ship/Port Interface
- Controlling access from the Waterfront and basic waterside patrol awareness.
- Basic search procedures for non-security personnel
- Case Study: Maersk Alabama Piracy Incident.

Module 6: Surveillance and Security Equipment

- Operational use and limitations of various Physical Security Equipment.
- Understanding and monitoring CCTV and other surveillance systems.
- Effective use of lighting, perimeter barriers, and intrusion detection systems.
- Basic procedures for calibration, testing, and maintenance of security systems.
- Case Study: False Alarm Management.

Module 7: Introduction to Maritime Cyber Security

- The increasing threat of Cyber-attacks on port IT and OT systems.
- Vulnerabilities in Operational Technology (OT)
- The importance of Cyber Hygiene
- Reporting protocols for suspected Data Breach or digital anomalies.
- Case Study: Major Shipping Company Cyber Incident.

Module 8: Response, Reporting, and Drills

- Protocols for reporting security incidents and suspicious activities.
- Understanding emergency procedures.
- The importance of mandatory Drills and Exercises for testing the security plan.
- Maintaining and auditing Security Records and documentation for compliance.
- Case Study: Black Sea Unmanned Vehicle Threat.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com