Advanced Port Security and ISPS Code Compliance Training Course

02 - 06 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #LOG4756_151267

Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of the International Ship and Port Facility Security (ISPS) Code and its critical role in modern maritime security. In an era of complex global threats, ensuring the security of port facilities is paramount to protecting international trade, national infrastructure, and human lives. This program is meticulously designed to move beyond theoretical knowledge, offering practical strategies for the implementation, management, and continuous improvement of port security systems. Drawing upon foundational principles and contemporary challenges, the curriculum is informed by the work of leading experts like Michael McNicholas, author of "Maritime Security: An Introduction". Participants will gain a robust understanding of the regulatory framework, risk assessment methodologies, and operational procedures required for full ISPS Code compliance. BIG BEN Training Center has developed this course to empower security professionals with the skills to conduct thorough security assessments, develop effective Port Facility Security Plans (PFSP), and lead security operations with confidence and competence, ensuring their facilities are prepared for any security eventuality.

Target Audience / This training course is suitable for:

- Port Facility Security Officers (PFSOs) and their deputies.
- Company Security Officers (CSOs) and Ship Security Officers (SSOs).
- Port and terminal managers and supervisors.
- Maritime security managers and consultants.
- Law enforcement and coast guard personnel involved in port security.
- Government officials and regulators in the maritime sector.
- Logistics and supply chain managers with security responsibilities.
- Corporate security and risk management professionals.
- Maritime operations personnel.

Target Sectors and Industries:

- Maritime and Shipping Industry.
- Port and Terminal Operations.
- Oil and Gas Sector (offshore and onshore terminals).
- Logistics and Supply Chain Management.
- Governmental agencies including Coast Guard, Navy, and Border Control.
- Private Maritime Security Companies.
- International Trade and Freight Forwarding.
- Cruise Line and Passenger Ferry Operations.

Target Organizations Departments:

- Security and Safety Departments.
- Port Operations and Management.
- Compliance and Regulatory Affairs.
- Risk Management and Internal Audit.
- Emergency Response and Crisis Management.
- Logistics and Supply Chain Operations.
- Human Resources and Training.
- Legal and Corporate Governance.

Course Offerings:

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

- Interpret the requirements of the SOLAS Convention and the ISPS Code accurately.
- Conduct a comprehensive Port Facility Security Assessment (PFSA).
- Develop, implement, and maintain a compliant Port Facility Security Plan (PFSP).
- Define the roles and responsibilities of a Port Facility Security Officer (PFSO).
- Manage the three security levels and implement appropriate protective measures.
- Plan, conduct, and evaluate effective security drills and exercises.
- Coordinate security activities with Ship Security Officers (SSOs) and Company Security Officers (CSOs).
- Effectively utilize security equipment and systems for port protection.
- Respond to security threats, breaches, and incidents in a structured manner.
- Prepare for and manage external audits and verification processes.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can directly apply their learning to their professional roles. We move beyond traditional lectures by integrating a dynamic blend of training techniques. The course heavily features detailed case studies of real-world maritime security incidents, allowing participants to analyze successes and failures in a controlled environment. Facilitated group discussions and brainstorming sessions encourage the sharing of diverse experiences and perspectives. Practical exercises, such as developing components of a Port Facility Security Plan or simulating a response to a security threat, are central to the learning process. Participants will work in teams to solve complex security problems, enhancing their decision-making and collaborative skills. Our expert instructors provide continuous feedback and guidance, fostering a supportive and challenging learning atmosphere that prioritizes skill mastery and operational readiness.

Course Agenda (Course Units):

Unit One: Foundations of Maritime Security and the ISPS Code

- Introduction to international maritime security policy.
- Historical context leading to the adoption of the ISPS Code.
- Understanding the SOLAS Convention Chapter XI-2.
- Key definitions and terminology within the ISPS Code.
- Roles and responsibilities of Contracting Governments and Designated Authorities.
- Detailed duties of the Company Security Officer (CSO) and Ship Security Officer (SSO).
- The central role and responsibilities of the Port Facility Security Officer (PFSO).

Unit Two: The Port Facility Security Assessment (PFSA)

- The purpose and objectives of the Port Facility Security Assessment.
- Methodology for conducting a comprehensive on-scene security survey.
- Identifying critical assets and infrastructure within the port facility.
- Threat identification and assessment for maritime operations.
- Identifying potential vulnerabilities in physical security, procedures, and personnel.
- Risk analysis and evaluation techniques.
- Documenting the PFSA and formulating recommendations.

Unit Three: Developing and Implementing the Port Facility Security Plan (PFSP)

- The mandatory requirements and structure of the Port Facility Security Plan.
- Developing procedures for access control to the port facility.
- Measures for securing restricted areas within the facility.
- Procedures for the secure handling of cargo and ship's stores.
- Monitoring techniques for the port facility and surrounding areas.
- Integrating security communication systems and protocols.
- Submission, approval, and amendment of the PFSP.

Unit Four: Practical Security Operations and Emergency Preparedness

- Implementing the three maritime security levels (MARSEC Levels 1, 2, and 3).
- Procedures for interfacing with ships and managing the Declaration of Security (DoS).
- Security awareness and vigilance training for all port personnel.
- Planning and conducting security drills and exercises effectively.
- Developing a robust security incident response plan.
- Coordination with local, national, and international security agencies.
- Managing media and communications during a security incident.

Unit Five: Auditing, Compliance, and Contemporary Security Challenges

- Techniques for conducting internal audits of security activities.
- Preparing the port facility for external verification and audits.
- Managing and rectifying non-conformities and observations.
- Record-keeping and documentation requirements for ISPS Code compliance.
- Recognizing and responding to emerging maritime threats.
- Introduction to maritime cybersecurity risks for port facilities.
- Best practices for continuous improvement of port security measures.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of increasing technological integration, how can port authorities balance the implementation of robust cybersecurity measures with the need for seamless, efficient cargo flow and data exchange?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the practical application of the ISPS Code within the complex operational reality of a modern port. While many programs cover the code's requirements, we emphasize the "how" and "why" behind effective security management. Our curriculum is built around a case-study methodology, dissecting real-world security breaches and successful interventions to provide actionable insights. We move beyond simple compliance, teaching participants how to build a resilient security culture that permeates all levels of the organization. The course content is continuously updated to address contemporary threats, including the growing challenge of cybersecurity in the maritime domain, ensuring the knowledge gained is relevant and forward-looking. Rather than just reciting regulations, our expert instructors, with their extensive field experience, facilitate a deep understanding of risk assessment and strategic planning. This approach transforms participants from passive learners into proactive security leaders capable of developing and managing a truly effective and compliant Port Facility Security Plan.