

ISM Code and Cyber Risk Management

Delivery Method: eLearning || Duration: 2 hour || Course Fee: 200 €

Category: Cybersecurity, Rules & Regulations, Shipping

Available languages: English

Certificate

On completion of the training program, the student will be awarded:

- A Certificate of **ISM Code and Cyber Risk Management**, issued by Bureau Veritas Solutions Marine & Offshore.

The Certificate of **ISM Code and Cyber Risk Management** is obtained after completing the course and passing the online test.

Presentation

This training course is about what an effective cyber security risk management should be. Its goal is not to address too many technical questions as the best technical expertise in the world won't guarantee zero cyber risk. The course aims at providing your Company with a real battle plan: know the assets, know the enemies, organize accordingly and train the effectives. Although this will not be enough to avoid a cyber incident, the severity of the consequences of a cyber incident will depend on the company's preparedness and ability to manage it.

Who the course is for

The course **ISM Code and Cyber Risk Management** is aimed at anyone interested in understanding how an effective cyber security risk management should be. This may include Top Management of Shipping Companies, Ship Managers, Technical Superintendents, Ship Masters, Officers and Seafarers; Offshore Units Operators and Technical Staff, Shipyards Technical Staff; Surveyors; P&I and/or Insurance Inspectors; etc.

Objectives

On completion of the training, students will be able to:

- Know what cyber security is, the main threats and their consequences.
- Understand how to consider the cyber risks in the Safety Management System and how the ISM Code translated into cyber security.
- Know the 12 cybersecurity commandments that will help implementing an efficient cyber risk management system.

Program

- Introduction
 - Consider cyber security as a business decision
 - What is cyber security exactly about?
- Shipping industry is a cyber target
 - Five reasons why you could be the next victim...
 - Four strategies to face cyber risks
- Cyber risk in Safety Management Systems
 - The NIST Framework
- Cyber security and ISM Code
 - Operational Technology (OT) and Information Technology (IT)
 - Risk analysis
 - Cyber security training
 - Training again... Procedures must be known and implemented
 - Crew training and awareness
 - Incident response procedures
 - Roles, rules and responsibilities
 - Cyber security policy
 - What should the cyber security policy include?
- Cyber security threats: Know your enemies!
 - Phishing (social engineering)
 - Malware
 - How to detect malware?
 - Ransomware (also known as Cryptolocker)
 - How to avoid ransomware?
 - In the case of ransomware
 - Spoofing
 - Identity theft
- 12 cyber security commandments