# Maritime Cyber Security Awareness: An Overview of the IMO Framework

**Mourad Ghorbel**
**Maritime and Port Security Expert**
**Maritime Safety Division**



INTERNATIONAL MARITIME ORGANIZATION

# Goal of Maritime Security

***Perfect security can never be fully realized. There exists no vessel or port facility that is so well protected it cannot be seized, damaged, or destroyed***.

***Risk Management, not Risk Elimination.***

So...why establish effective Maritime Security?

# Goal of Maritime Security

- To make access to the target so difficult as to **discourage/deter the attempt**.
- Put measures in place to **harden** ship/port facility attack.
- To ensure the **attempt remains an attempt**.
- And, if the attempt is made, to **minimize the damage**.

# Goal of Maritime Security

## In Order To Achieve This….

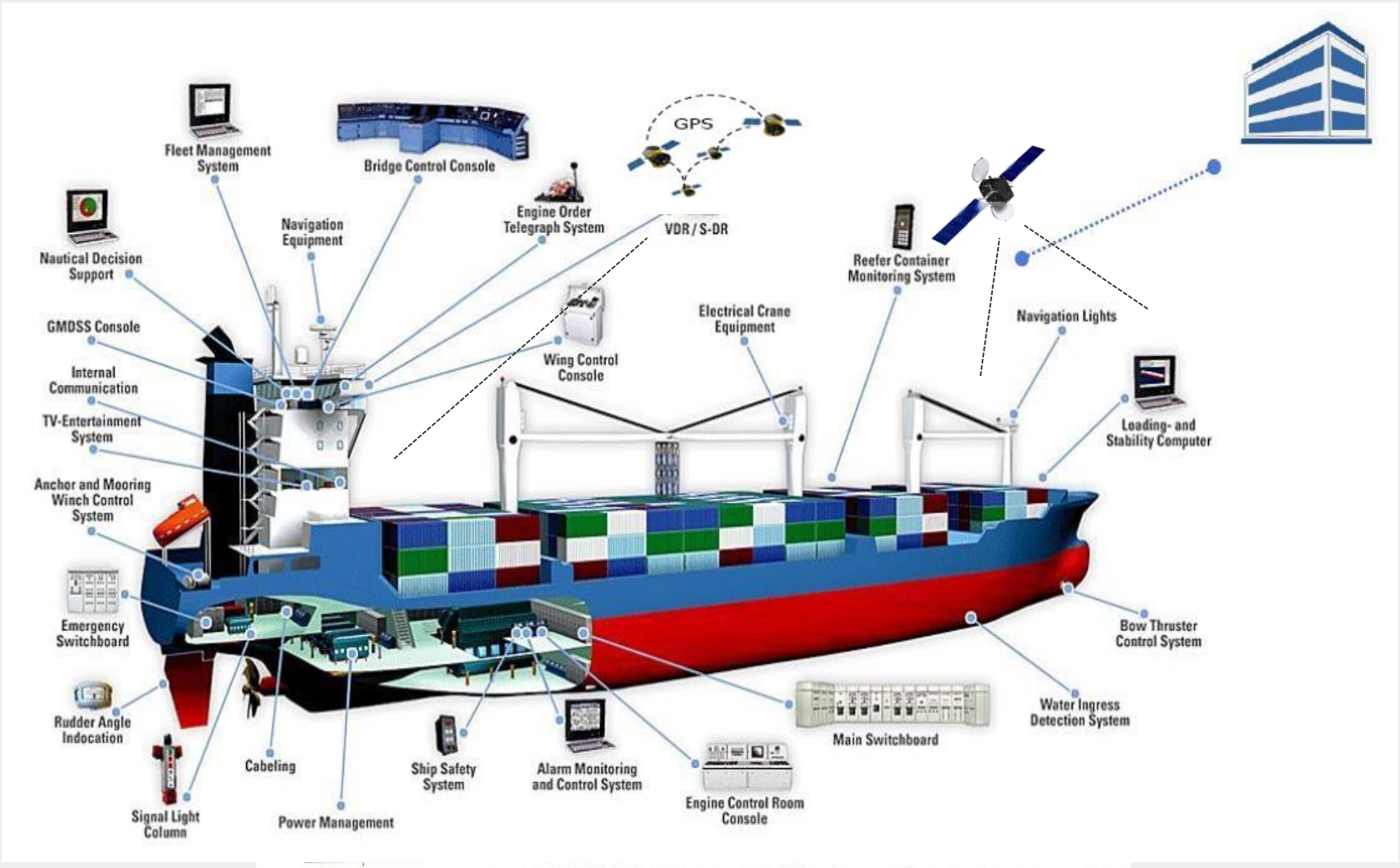
- First - Understand the Maritime Threats
- Then - Develop Measures & Appropriate Responses to Detect & Deter the Threats.

*"Know Thy Enemy, Know Thyself, A Hundred Battles Fought,*
*A Hundred Battles Won"*
*Sun Tzu*

# Why do cyber incidents happen?

# AN INCREASINGLY DIGITISED SHIP

IT & OT SYSTEMS ONBOARD



# Networking on board

Networking environment in a simple merchant ship: Usually at least 2 or 3 different networks

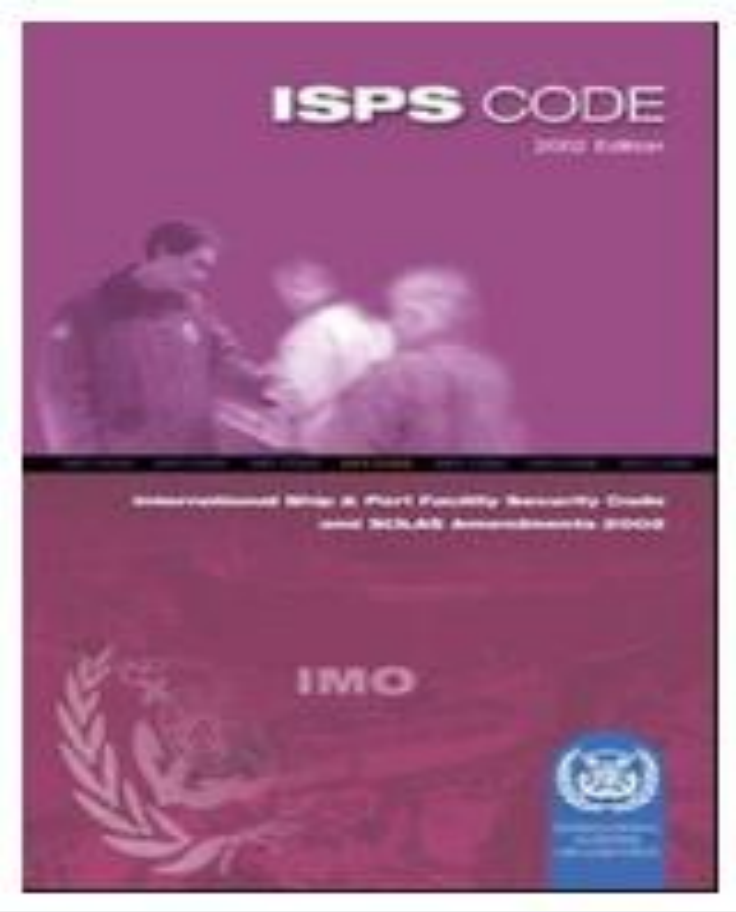
- ✓ **Crew** one get also personal devices
- ✓ **Business** are from 10 to 20 devices, servers, PC`s and voip phones
- ✓ **Systems** means for example navigation systems like EGDIS, 24/7 connected to get updates.

# Port Facilities

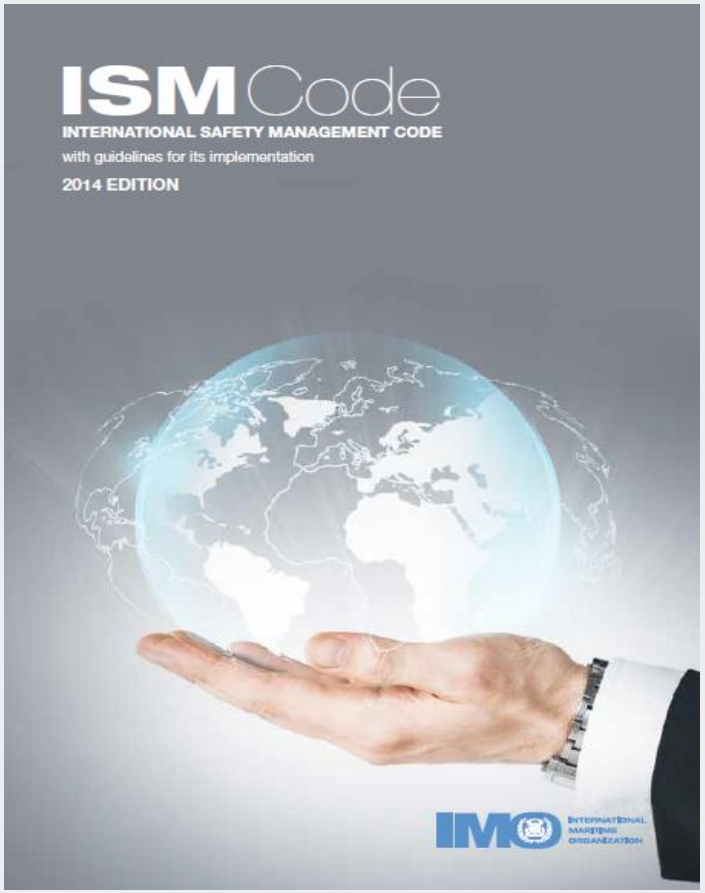
- Networked computer and control systems integral to almost everything…


# What is the IMO framework related to cyber threats ?

# Legal Framework/ Mandatory Instruments

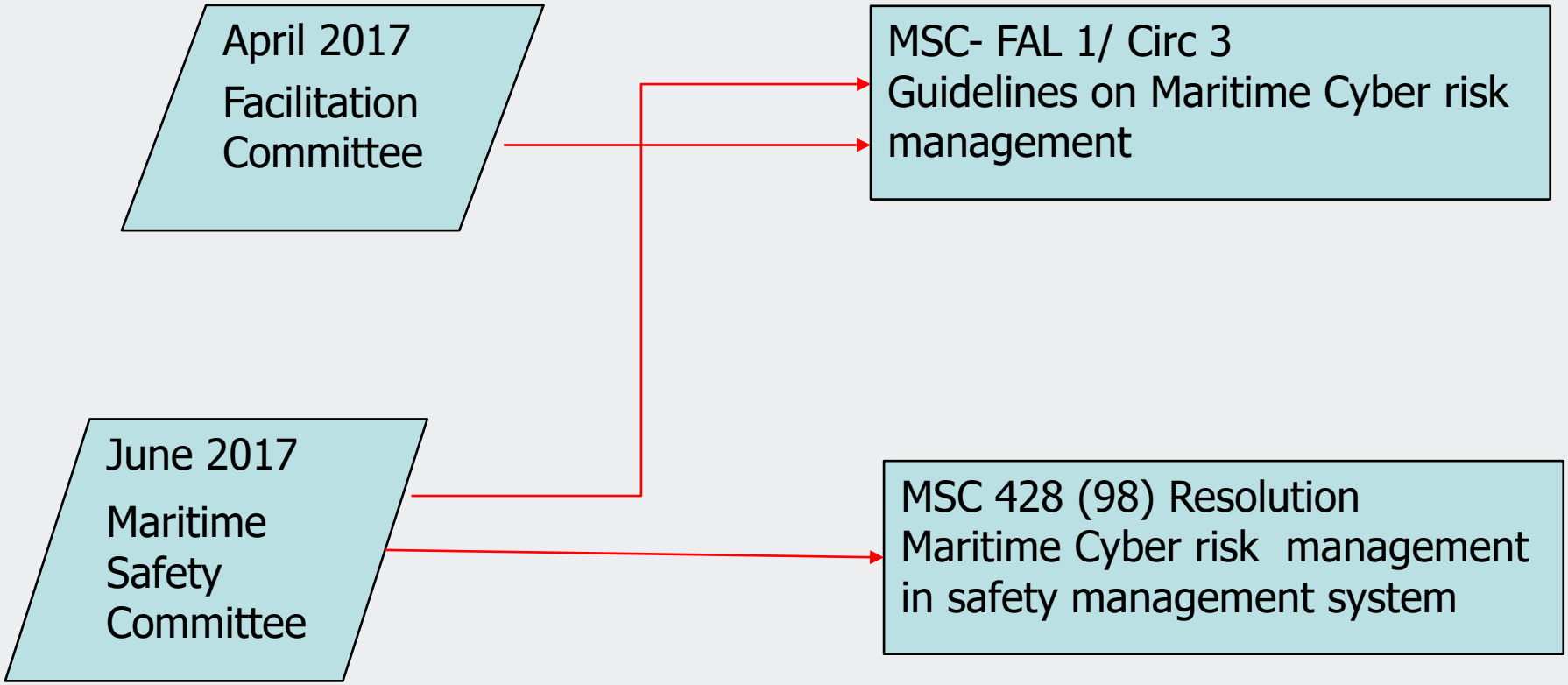



2002



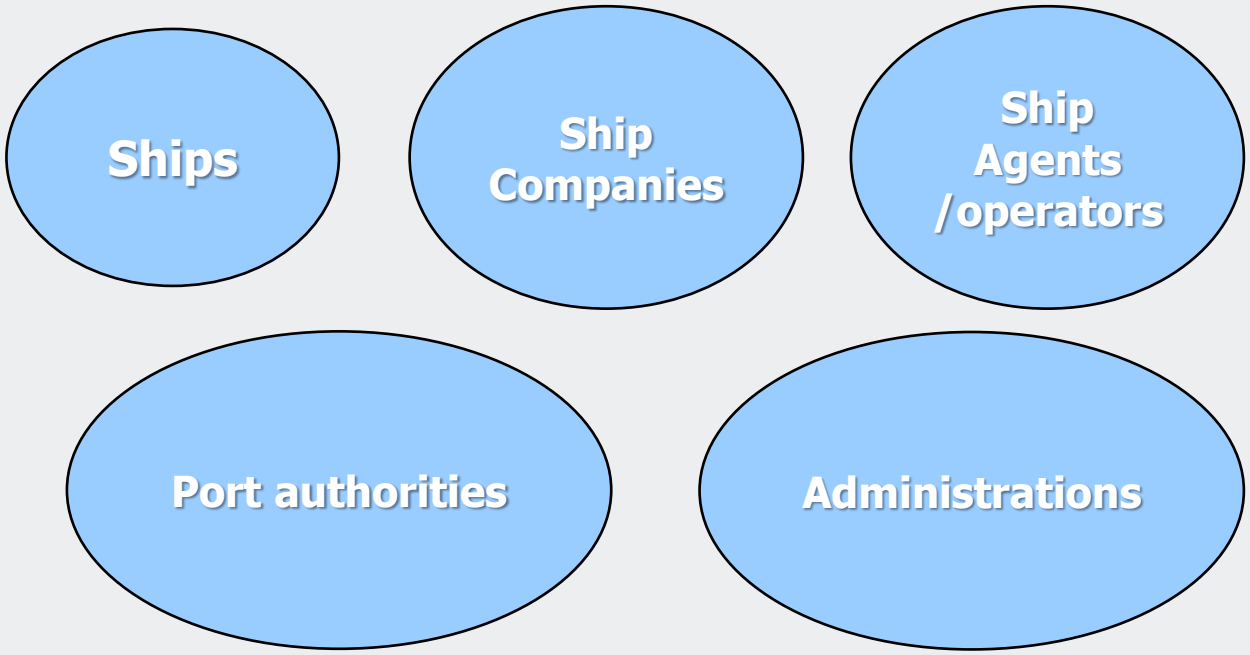

1993

# IMO Guidelines



# Who is MSC-FAL.1/Circ.3 for?

The **Guidelines on maritime cyber risk management** are primarily intended **for all organizations in the shipping industry**, and are designed to encourage safety and security management practices in the cyber domain.



# Maritime cyber risk

**Maritime cyber risk** refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

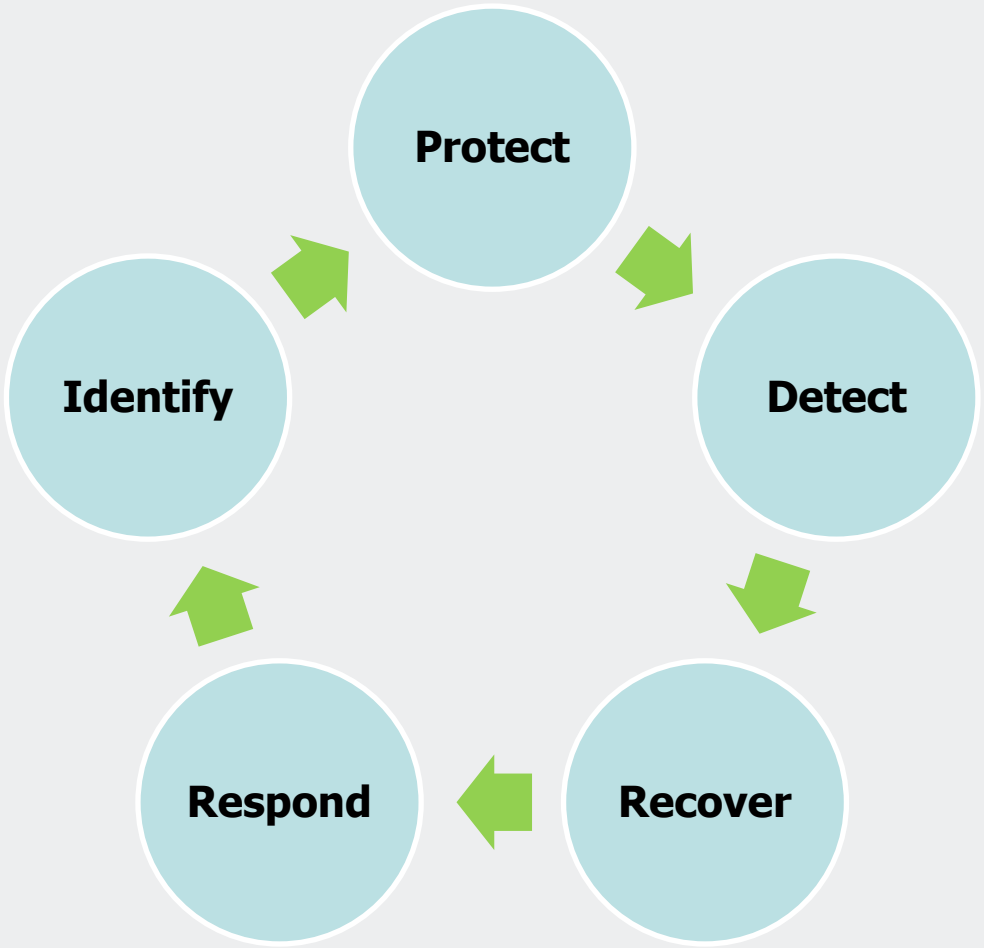
**Maritime Cyber Risk**

# Maritime cyber risk management

**Cyber risk management** means the process of **identifying, analysing, assessing and communicating** a cyber-related risk and **accepting, avoiding, transferring or mitigating it to an acceptable level**, considering costs and benefits of actions taken to stakeholders.

The **Overall goal** is to **support safe and secure shipping**, which is operationally resilient to cyber risks.

# Effective cyber risk management

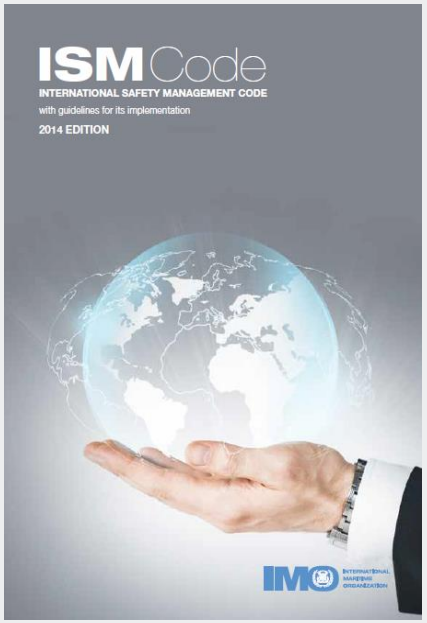


# Maritime cyber risk management

Additional guidance and standards may include:

- The **Guidelines on Cyber Security on board Ships** by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- **ISO/IEC 27001 standard on Information technology** – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (**the NIST Framework**).
- UK DfT Cyber Security Codes of Practice for Ships and Ports

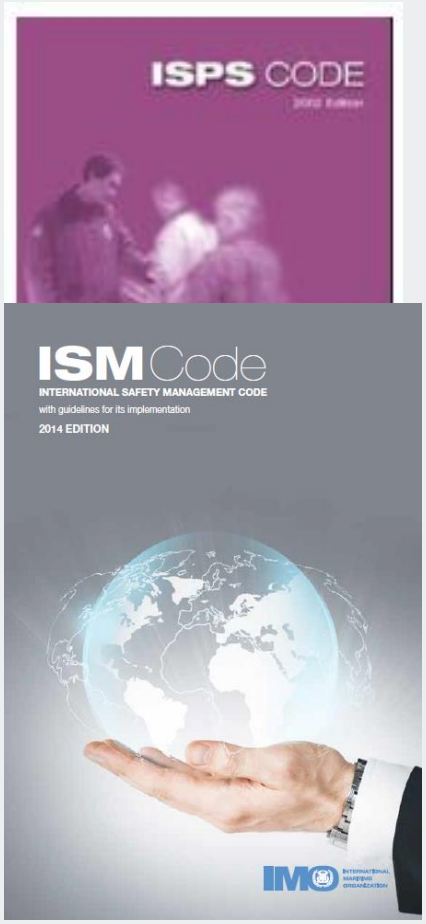
# Resolution MSC.428(98)




The Maritime Safety Committee, in June 2017:

- Affirmed that an approved **safety management system should take into account cyber risk management** in accordance with the objectives and functional requirements of the ISM Code;
- Encouraged Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after **1 January 2021**;
- Acknowledged the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management

# Clarifications at MSC 101 in 2019




- Agreed that aspects of cyber risk management, including physical security aspects of cyber security, should be addressed in Ship Security Plans under the ISPS Code; however, this should not be considered as requiring a company to establish a separate cyber security management system operating in parallel with the company SMS;
- Confirmed that resolution MSC.428(98) on Maritime cyber risk management in Safety Management Systems set out the Organization's requirements for Administrations to ensure that cyber risks were appropriately addressed in existing SMS (as defined in the ISM Code), verified by an endorsed Document of Compliance and Safety Management Certificate, and that in the Ship Security Plan, reference should be made to cyber risk management procedures found in SMS.

# ISPS Code/ Cycle of cyber risk management


SSA / PFSA

Ship Security Assessment (SSA) / Port Facility Security Assessment (PFSA) :
Documents which inter alia identifie weakness of the ship / PF (including human factors, assets, policies and procedures) in term of security

SSP/ PFSP

Ship Security Plan (SSP) / Port Facility Security Plan ( PFSP) :
Plans developed to address the risks identified in the assessment phase.

# ISPS Code / SSA

**( ISPS Code Part A section 8.4)**

SSA shall include at least:

1- identification of existing security measures, procedures and operations.

2- identification and evaluation of **key shipboard operations that it is important to protect.**

3- **identification of possible threats** to the key shipboard operations and the likelihood of their occurrence.

4- **identification of weaknesses** including humain factors, in the infrastructure, policies and procedures

# ISPS Code / SSA

**( ISPS Code Part B section 8.3)**

SSA shall address the following elements on board or within the ship:

- Physical security;
- Structural integrity**;**
- Personal protection systems;
- Procedural policies;
- Radio and telecommunication systems including computer systems and networks; and
- Other areas that may, if damaged pose a risk to persons, property, or operations on board the ship

# ISPS Code / PFSA

**( ISPS Code Part A section 15.5)**

The PFSA shall include, at least the following elements:

- Identification and evaluation of important assets and infrastructure it is important to protect;
- Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence
- Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and
- Identification of weaknesses including human factors in the infrastructure, policies and procedures.

# ISPS Code / PFSA

**( ISPS Code Part B section 15.3)**

PFSP should address the following elements within the Port Facility:

- Physical security;
- Structural integrity**;**
- Personal protection systems;
- Procedural policies;
- Radio and telecommunication systems including computer systems and networks;
- Utilities; and
- Other areas that may, if damaged pose a risk to persons, property, or operations within the port facility

# PEOPLE ARE THE KEY

IT IS NOT ONLY ABOUT PROCESS AND TECHNOLOGY

## PEOPLE

- **Training & awareness**
- **Professional skills & qualifications**
- **Written procedures**
- **Authorizations**
- **Physical security**

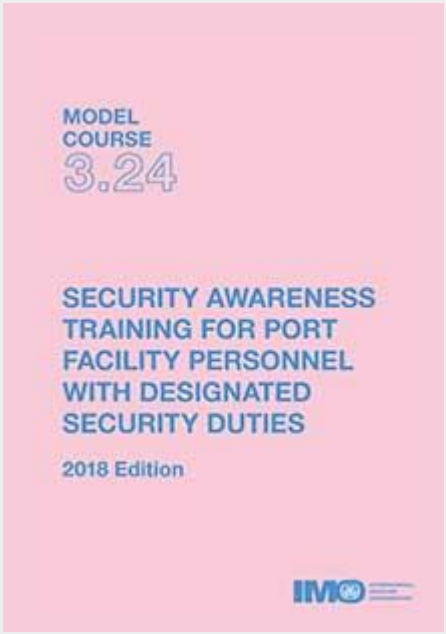
## PROCESS

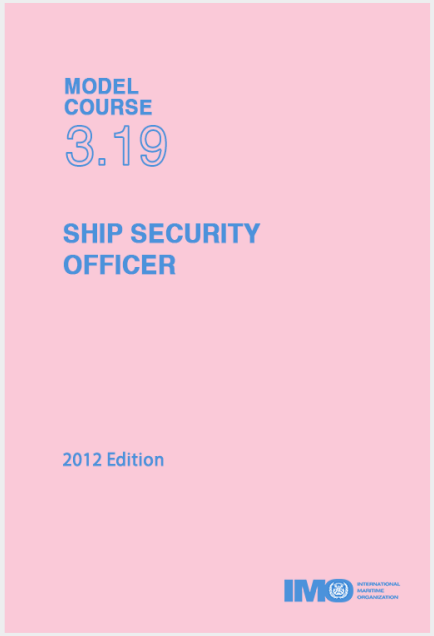
- Management Systems
- Governance Frameworks
- Policies & procedures
- Vendor/third party contracts-follow up
- Audit regimes

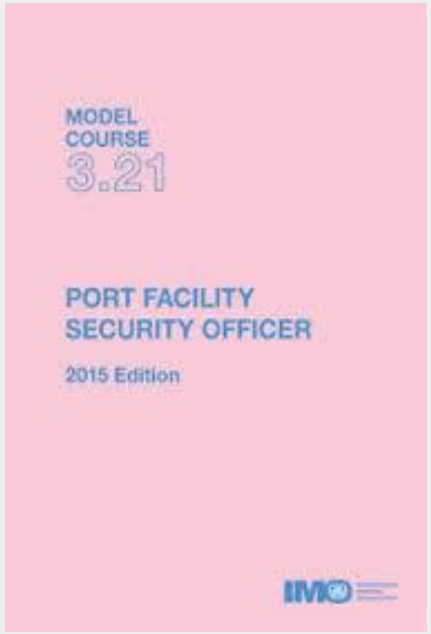
## TECHNOLOGY

- System design, design review
- Software configurations
- Inspection/verification
- Testing
  - Functional testing
  - Vulnerability scanning
  - Penetration test

# Training of seafarers and shore-based Personnel




IMO is updating its security model courses to incorporate maritime cyber risk management.

## International Maritime Organization


4 Albert Embankment
London
SE1 7SR
United Kingdom

Tel: +44 (0)20 7735 7611
Fax: +44 (0)20 7587 3210
Email: info@imo.org
**www.imo.org**





twitter.com/imohq facebook.com/imohq youtube.com/imohq flickr.com/photos/imo-un/collections