Dr. Theodoros Ntouskas

Managing Director, ictPROTECT

Maritime Cybersecurity Compliance Roadmap

13ο InfoCom Security
26 & 27 Απριλίου 2023

ictPROTECT
INFORMATION SECURITY SERVICES

www.ictprotect.com

Floating Digital Offices

ict PROTECT
INFORMATION SECURITY SERVICES

Bridge Officers

Crew

Maritime Company Users

Navigation Services (AIS, GPS, ECDIS)

Communication Systems

Operational Services

Cargo Management

PMS

Crew network

OT Equipment

Commercial Ships & Cybersecurity Requirements

ict PROTECT
INFORMATION SECURITY SERVICES

IMO IMO's MSC-FAI.1-Circ.3

Classification Soc. Cyber secure class notation

TMSA3

BIMCO

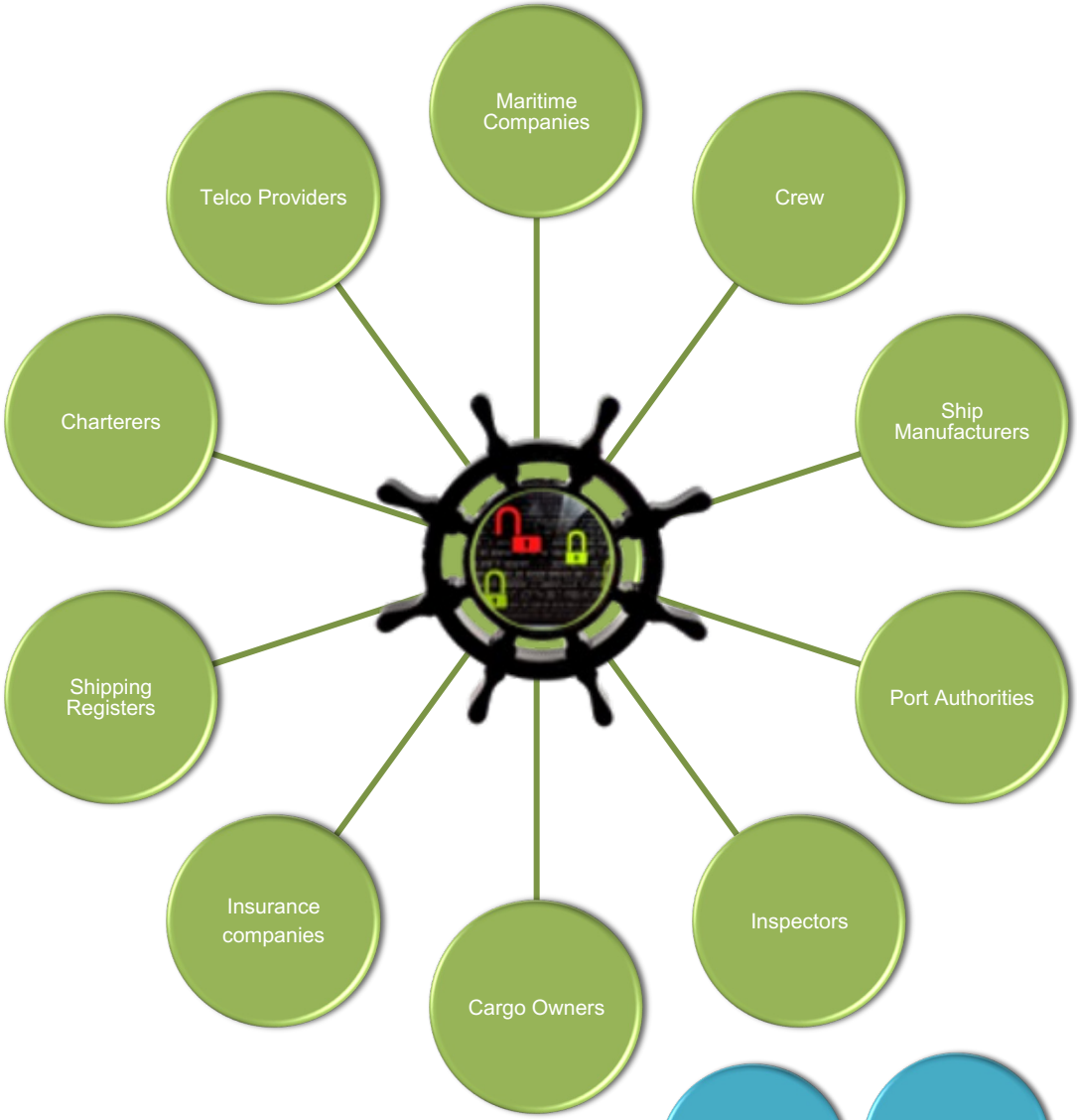
Us Coast Guard, Feb. 2020

IACS, rec.166

ENISA

UK DfT

IAPH



ISO 27001

ISO 22301

ISO 27701

SOC 2

GDPR

CCPA

ISO 27002

NIST CSF

Requirement

Class Notation

Guideline

Standard

Port Guideline

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase I:
Define Cyber Security Team

-- Appoint CySo

-- Assign security responsibilities to key personnel

Goals

Assign security responsibilities to key personnel (i.e. Master, Crew, Security

Engineers, Department Managers)

Ensure Accountability

Responsibilities for the assets

Risks

Asset ownership related risks

Non-repudiation related risks

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase II: Cartography

-- Identify Information Assets (IT & OT)
-- Identify assets' dependencies
-- Identify the core business requirements
-- Identify key suppliers

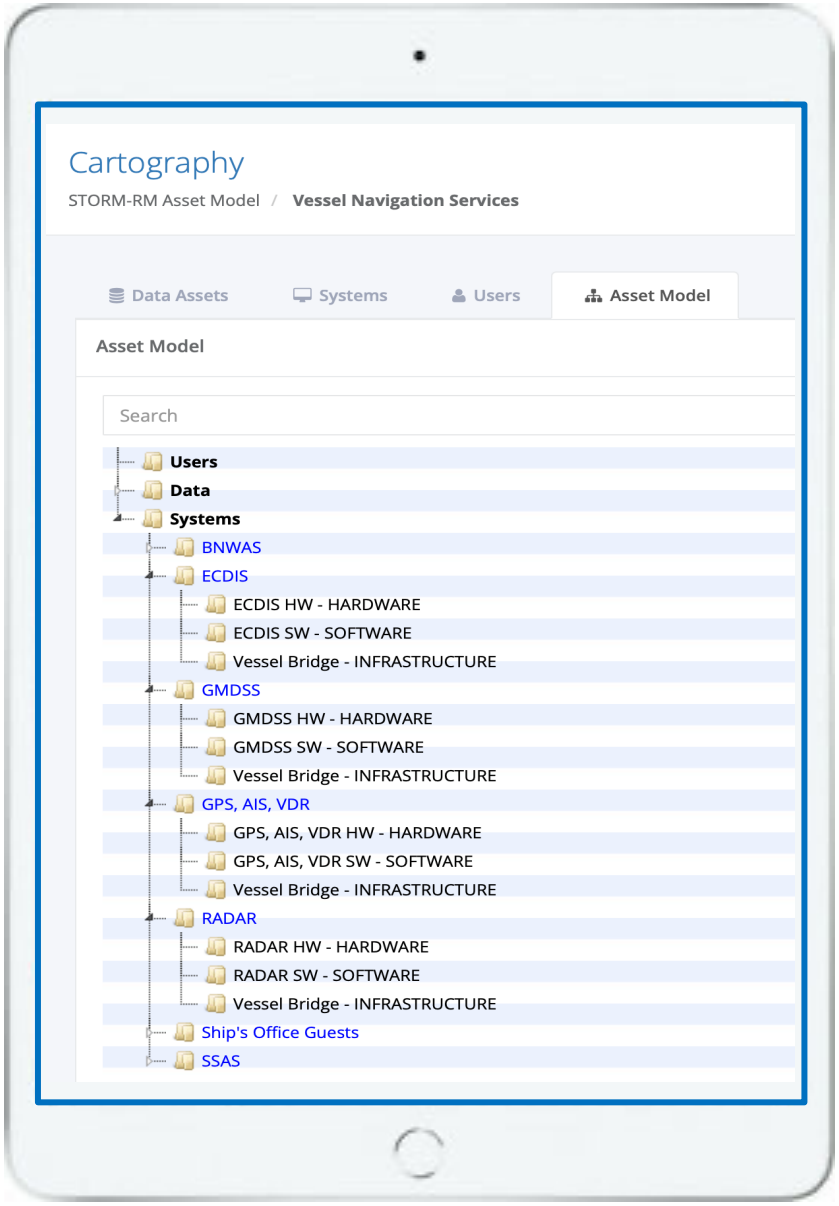
Goals

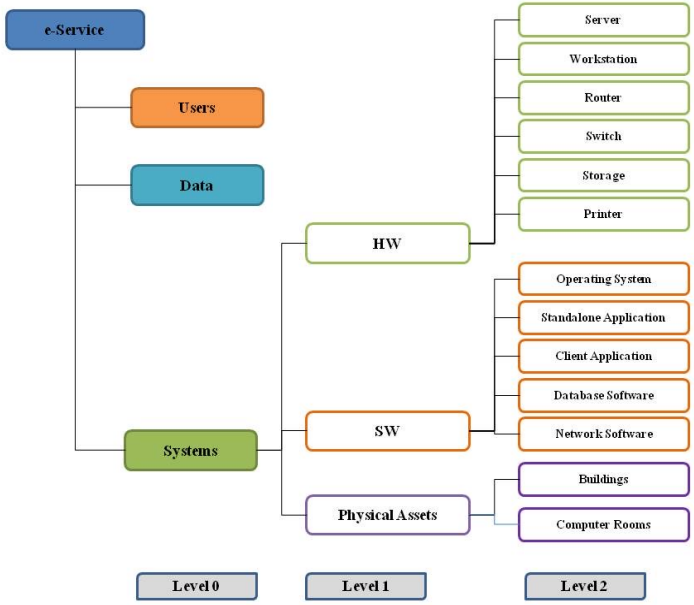
Identify asset (IT/OT) dependencies
Identify services dependencies
Accurate list of critical suppliers
Accurate impact assessment
Targeted threat scenarios

Risks

Inaccurate asset inventory
Loss of dependencies
Unwanted services / assets

Vessel IT&OT Asset Model





Our Proposed Compliance Methodology

Phase III: Conduct Readiness Assessment

-- Map ISO 27001 & NIST controls with best practices such as IMO,ISM Code, TMSA, BIMCO etc.

-- Identify existing controls and find grey areas

Goals

Promptly identify grey areas

Create a compliance baseline

Improve reporting for interested parties

Risks

Compliance risks

Non compliance with interested parties requirement

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase IV: Evaluate Key Suppliers

-- Evaluate their technical controls

-- Evaluate Supported Services - SLAs & DPA

-- Compliance with applicable regulation

Goals

Confirm provided SLA

Comply with legal requirements

Assign security related responsibilities to critical suppliers

Establish a common framework for evaluating suppliers

Require cyber risk management procedures from suppliers

Risks

Supply chain risks

Technical risks during maintainance phase

Not established communication lines / escalation matrix during incidents

Digital supply chain risk

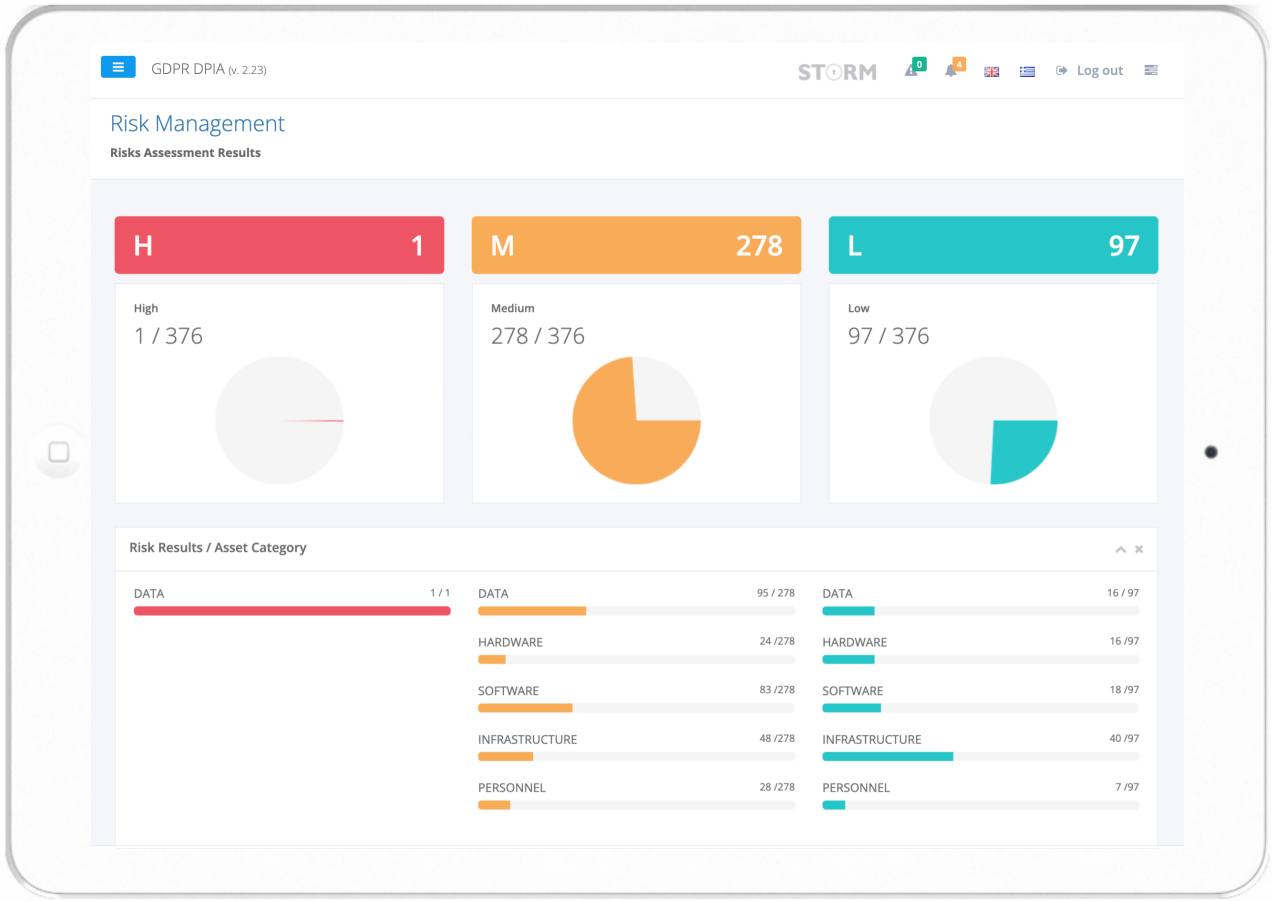
-- Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase V: Conduct Risk Assessment & Risk Treatment

- Impact Assessment
- Identify Potential Threats
- Evaluate Vulnerabilities
- Propose Mitigation Actions



Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase VI: Develop technical & organizational controls

-- Security Policies & Procedures – embedded in the existing Manual

-- Hardening of IT & OT equipment

Goals

- Adopt security policies & procedures by all employees
- Common language across company departments
- Establish cybersecurity incident plans
- Establish a holistic approach to cybersecurity including IT & OT systems
- Hardening and automation as possible

Risks

- Miscommunication across company users
- Unpatched systems

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase VII: Develop Contingency Plans

-- Identify recovery priorities

-- Identify dependencies (SLAs with key suppliers & DPA with data processors)

-- Establish communication lines

-- Create Runbooks in case of unwanted event

Goals

Implement a comprehensive Cyber security incident framework

Assign ashore and at sea the appropriate responsibilities in case of an incident

Establish communication lines

Evaluate and improve recovery steps

Risks

Miscommunication during incident management

Loss of data / service due to supplier failure

Insufficient recovery priorities

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Phase VIII: Monitor, Audit & Review

-- Internal audit

-- Review technical & organizational controls

Goals

Identify grey areas & areas of non-conformity on time

Propose areas for improvement

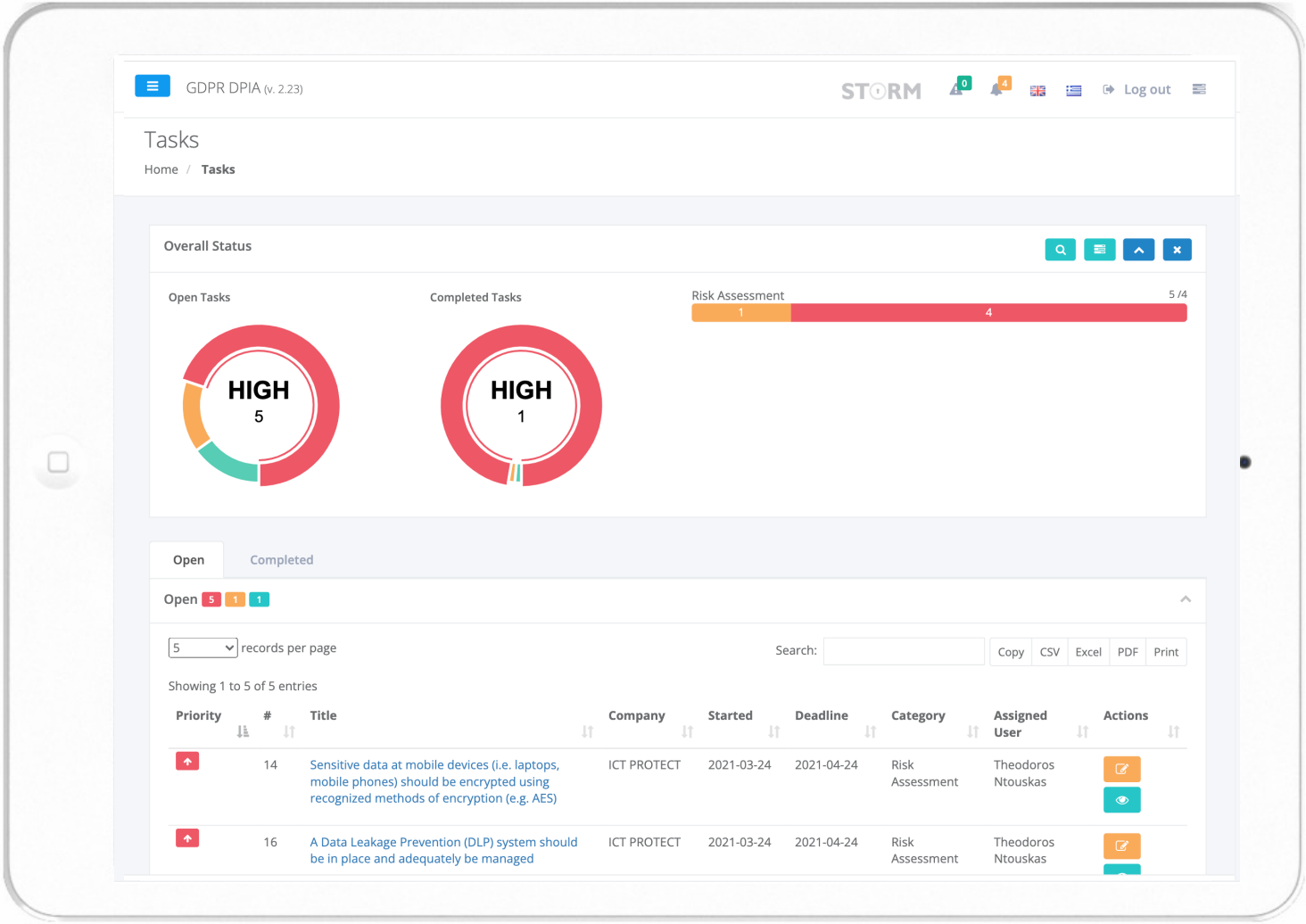
Identify the appropriate corrective actions

Risks

Non compliance with industry standards

Non compliance with company standards

Non compliance with interested parties requirements



General Conclusions and Proposals

- With the **rapid growth** and adoption of technology in maritime environment, **Ship Information Systems (SIS)** and **Port ICT** are increasingly exposed against cyber risks.

- These cyber risks could be exploited:
  - by **satellite networks**, either
  - by **the traditional communication channels**
- and could have **significant impact** on all **maritime entities** affecting **international economy**.

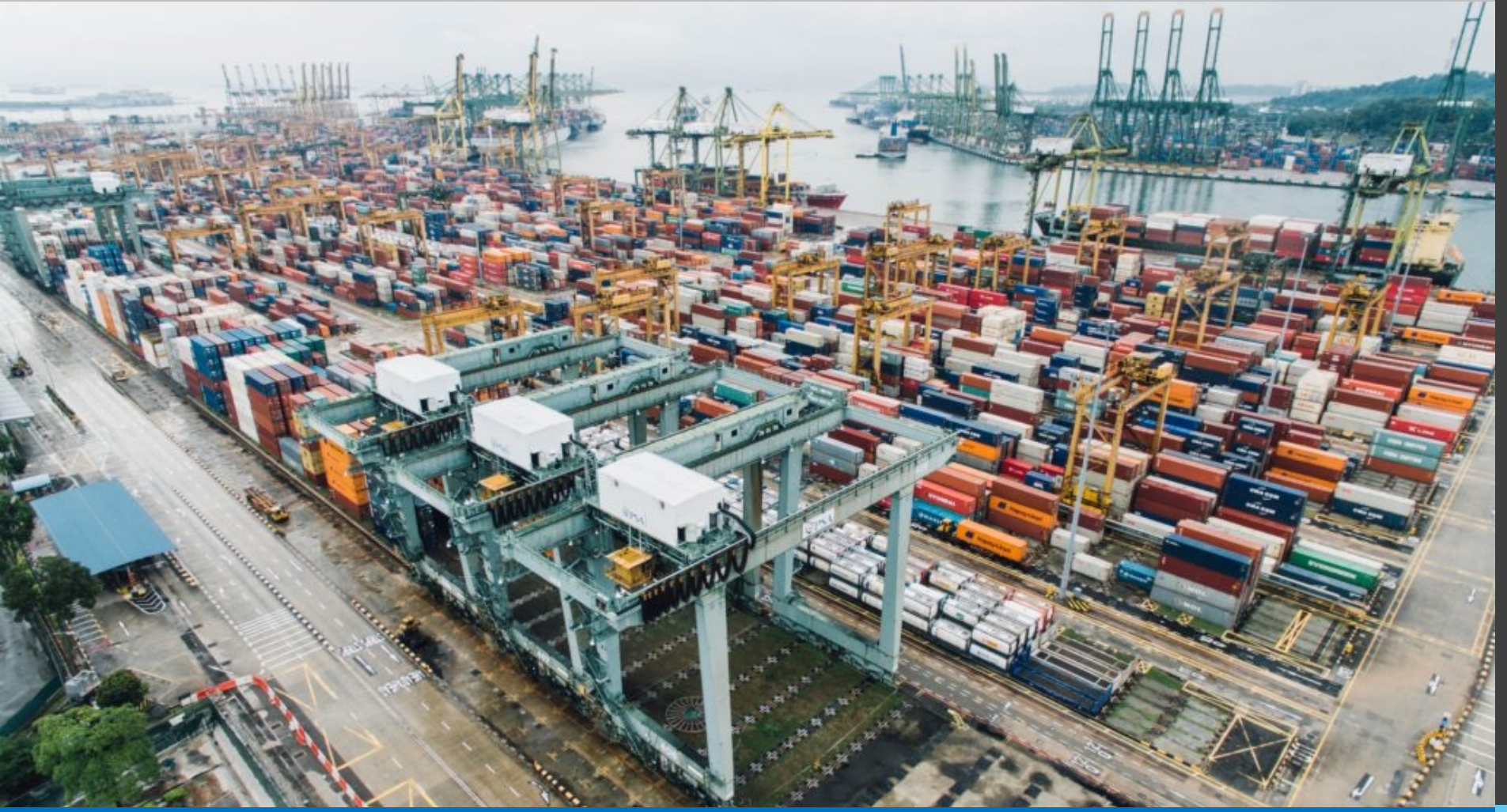
- New & complex **compliance requirements**

- A **holistic and common approach (Cybersecurity Compliance Framework**) should be adopted for the security management of both ICT & OT systems in order to:
  - continuously monitor security and privacy risks,
  - improve their ICT-based business processes,
  - provide continuity and rendering of services for all entities of the maritime environment

References

- IMO - MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management, July 2017,
  - https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
- IMO - RESOLUTION MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, June 2017,
  - https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
- United States Coast Guard, February 2020, Guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities,
  - https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023
- IACS (International Association of Classification Societies (IACS)) UK, Rec 166 - Recommendation on Cyber Resilience - New Corr.1 July 2020 Clean,
  - https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/ https://iacs.org.uk/download/10965
- OCIMF - TMSA3 - Tanker Management Self-Assessment, April 2017,
  - https://www.shipnet.no/key-elements-of-tmsa-3/
- BIMCO - The Guidelines on Cyber Security Onboard Ships v4,
  - https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- BIMCO - Cyber Security Workbook for On Board Ship Use, 2nd Edition, 2021,
  - https://www.bimco.org/about-us-and-our-members/publications/cyber-security-workbook
- BIMCO- The Guidelines on Cyber Security Onboard Ships
  - https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- IMO – ISM Code, 2018 Edition,
  - https://www.dohle-yachts.com/wp-content/uploads/2021/05/ISM-Code-2018.pdf
- ENISA – EU, Port Cybersecurity – Good practices for cybersecurity in the maritime sector, November 2019,
  - https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
- United Kingdom Department of Transport - Cyber Security for Ports and Port Systems, January 2020,
  - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf
- IAPH – International Association of Ports and Harbors, Port Community Cyber Security,
  - https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf
  - https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

Introduction - Our services



Let’s do business

info@ictprotect.com

ict PROTECT
INFORMATION SECURITY SERVICES