EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBER RISK MANAGEMENT FOR PORTS

Guidelines for cybersecurity in the maritime sector

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Dr. Athanasios Drougkas, Anna Sarri, Pinelopi Kyranoudi, EU Agency for Cybersecurity

ACKNOWLEDGEMENTS

For providing valuable information that helped shape the report (in alphabetical order):

Peter Alkema, Strategic Policy Advisor and Project Manager, Harbour Master's Office, Port of Amsterdam

Sylvie Andraud, Maritime Sector Coordinator, The National Cybersecurity Agency of France (ANSSI)

Jérôme Besancenot, CIO, HAROPA Port of Le Havre

Javier Castillejo Reyes, Head of Maritime Safety&Security Unit, Spanish Maritime Administration

Rafael Company, Director of Safety and Security, Fundación Valenciaport

Joost Daem, CISO, PSA Antwerp

Neil Davis, Head of Cybersecurity Risk Management, A.P. Moller Maersk

Chris Day, Senior Cybersecurity Consultant - OT, A.P. Moller Maersk

Aymeric de Marcellus, Senior Project Officer, Unit Safety & Security / Department Safety, Security and Surveillance, EMSA

Simone Fortin, Head of Cybersecurity, MSC Cruises

Luca Gargano, Project Officer for Maritime Security - Unit Safety & Security / Department Safety, Security and Surveillance, EMSA

Amol Ghatol, Cybersecurity Risk Manager, A.P. Moller Maersk

Soren Martin Hansen, Port Inspector, Danish Transport, Construction, and Housing Authority

Yannick Herrebaut, Cyber Resilience Manager - CISO, Port of Antwerp

Lance Kaneshiro, Chief Information Officer, Port of Los Angeles

Indrek Korela, Information Security Manager, Port of Tallinn

Niels Martin Madsen, Head of Section, Department for Aviation & Railway Security, Cyber- and Information Security Unit (DCIS), Danish Transport, Construction, and Housing Authority

Ilias Manos, IT Security Officer, Piraeus Port Authority

Flavio Marangi, CyberSecurity and Space Officer, Italian Ministry of Infrastructure and Transport - Central Security Unit

Ethan Moore, Cybersecurity Risk Manager, A.P. Moller Maersk

Machiel Noijen, Safety & Security Advisor, Harbour Master's Office,, Port of Amsterdam

Ruben Panés Butrón, Project Officer – Unit Safety & Security / Department Safety, Security and Surveillance, EMSA
Ricardo Pinto, IT Security Officer, PSA Sines
Díaz Puyol María del Carmen, Marine Surveyor, Barcelona Harbour Master Office
Jan Schirrmacher, Port Cyber Security Officer, Bremenports
Ward Veltman, Cyber Security & Risk Officer, Port of Rotterdam
Belle Webster, Head of IT and Cybersecurity, Port of Amsterdam

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-403-9 - DOI 10.2824/671060

TABLE OF CONTENTS

FIGURES AND TABLES

TABLES

FIGURES

EXECUTIVE SUMMARY

Over the last few years EU port operators have started to gradually address cyber risks as part of their security risk management processes in a more systematic manner. However, contrary to traditional security risk management, addressing cyber risks introduces entirely new challenges for port operators who often lack the internal expertise, organisational structure and processes or the resources to effectively assess and mitigate them. Moreover, the nature of port operations and, especially, the interconnectedness and service inter-dependencies across port ecosystems requires all involved operators to achieve and maintain a baseline level of cybersecurity.

This report aims to provide port operators with good practices for cyber risk assessment that they can adapt to whatever risk assessment methodology they follow. In order to achieve this, this report introduces a four-phase approach to cyber risk management for port operators, which follows common risk management principles and is mapped to the steps of the risk assessment methodology that is laid out in the ISPS Code[1] and relevant EU legislation for Port and Port Facility Security.

Specifically, the four phases are:

- Phase 1: Identifying cyber-related assets and services
- Phase 2: Identifying and evaluating cyber-related risks
- Phase 3: Identifying security measures
- Phase 4: Assessing cybersecurity maturity

For each of these phases, this report provides **actionable guidelines** to assist port operators in their efforts, lists common **challenges** associated with the performance of the relevant activities, **good practices** that can be readily adopted and customised by individual organisations and a **mapping of the listed good practices for each phase with the respective challenges** they address. The proposed guidelines and good practices may be adapted to any common cyber risk management methodology and can be tailored to the unique characteristics of port operators of different sizes, cybersecurity maturity, information security budgets and operational scope.

Phase four of this approach also introduces a model for port operators to perform cybersecurity maturity self-assessment founded on the selected security measures and to identify priorities for investing resources for either improving on or building an organisational cybersecurity maturity program.

[1] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

1. INTRODUCTION

Ports serve a critical function in facilitating domestic and international supply-chain activities by connecting sea and inland transport services. In the EU seaports play a significant role, supporting 90 percent of EU exports and an additional 43 percent of internal market exchange[2]. Ports are considered as critical information infrastructure for water transport. The **Directive 2016/1148 (NIS Directive)[3]** classifies m*anaging bodies of ports* (defined as "any specified area of land and water, with boundaries defined by the Member State MS in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations" in the Directive 2005/65/EC[4]), including *their port facilities* (defined as "a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate" in the Regulation (EC) No 725/2004[5]) and *entities operating works and equipment* contained within ports as eligible to be identified as Operators of Essential Services (OES).

This report builds on the *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector* report[6] published in November 2019 by ENISA, the EU Agency for Cybersecurity and provides additional guidelines to port operators for managing their cyber risks.

1.1 BACKGROUND

The NIS Directive requires OES to conduct risk assessments that "**cover all operations including the security, integrity and resilience of network and information systems**"[7]. According to the NIS Directive, these risk assessments, along with the implementation of appropriate mitigation measures, should promote "**a culture of risk management**" to be developed through "appropriate regulatory requirements and voluntary industry practices"[8]. While some EU Member States (MS) have issued relevant guidance to port operators on how to conduct cyber risk assessment (see Annex A for reference), most port operators have chosen to adopt one of the different methodologies introduced in the various industry standards (see Annex B for reference). However, there is no common methodology for port cyber risk assessment.

Of the three types of port OES defined in the NIS Directive, the closest framework to a common risk assessment methodology is the **International Maritime Organisation's International Ship and Port Facility Security (ISPS) Code**, which concerns port facilities / terminal operators. The ISPS code is implemented in the EU by Regulation 725/2004 and ensures that port facilities implement **Port Facility Security Assessments (PFSAs)** and **Port Facility Security Plans (PFSPs)**. The ISPS Code focuses primarily on physical security, though Part B, paragraph 15.3.5 of the Code recommends that the PFSA address computer systems and networks. It further specifically identifies radio and telecommunication systems, including computer systems and networks, and associated procedural policies. The ISPS code also defines minimum port facility security assessment elements/steps. EU **Directive 2005/65 on enhancing port security[9]** introduces similar requirements and extends them to ports, namely with the

[2] https://ec.europa.eu/transport/modes/maritime_en
[3] See https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148
[4] See https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:FR:PDF
[5] See https://eur-lex.europa.eu/legal-content/En/TXT/?uri=CELEX%3A32004R0725
[6] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
[7] See paragraph (13) page L.194/3 of https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[8] See paragraph (44) page L.194/8 of https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0065

implementation of **Port Security Plans (PSP)** and **Port Security Assessments (PSA)**. These measures should apply to all ports in which one or more port facilities covered by Regulation (EC) No 725/2004 are situated. Annex I of the Directive describes the minimum requirements for conducting a PSA in the same manner as Regulation 725/2004. PSAs shall take due account of the specificities of different sections of a port and, where deemed applicable by the relevant authority of the MS, of its adjacent areas if these have an impact on security in the port and shall take into account the assessments for port facilities within their boundaries as carried out pursuant to Regulation (EC) No 725/2004.

Stocktaking for this report revealed that a fragmented approach in the performance of cyber risk assessments occurs across the EU port sector. Almost without exception, each port's attempt to address cyber risk within context of existing security risk assessment frameworks and standards, followed a unique approach. Even more, port facilities complying with ISPS Code requirements indicated that significant gaps emerged in their organisational cyber risk assessments. Inconsistent approaches represented only half the challenge. Key aspects of organisations were left un-assessed due to a variety of factors that included but were not limited to port resource availability and variability, variations in stakeholder knowledge and degrees of engagement, compliance based focus, and inconsistent perceptions in how cyber risk can affect a port facility's operations.

1.2 STUDY OBJECTIVES

This report aims to provide port operators with a set of guidelines and good practices to effectively manage commonly referenced cyber risk management challenges. Specifically, the objectives of this report are established to provide port operators with:

- Good practices for cyber risk assessment that can be adapted to a range of risk assessment methodologies;
- Actionable guidelines that make effective use of the taxonomies (e.g. assets, threats etc.) presented in the 2019 ENISA report; and,
- A framework for identifying appropriate cybersecurity measures to address cyber risks and to conduct a cybersecurity maturity self-assessment that will facilitate the development, prioritisation, and efficient allocation of cybersecurity budgets.

1.3 STUDY SCOPE

- This study outlines good practices for cyber risk management in the maritime port ecosystem concerning both IT systems and OT systems.
- The port ecosystem comprises all the stakeholder groups involved in port operations: port managing bodies (Port Authorities, terminal and facility operators), national authorities (customs, police, cities, etc.), transport companies (shipping companies, railway companies, etc.) and all the service providers essential to port operations (oil companies, energy companies, etc.).

1.4 TARGET AUDIENCE

The primary target audience of this study are **people responsible for cybersecurity** (CISOs**,** CIOs etc.) within operators in the port ecosystem, namely

- Port Authorities;
- Port facilities / terminal operators;
- Other entities operating within ports.

In addition, the study can be useful for National Competent Authorities who may wish to develop guidance for port operators to support them in conducting cyber risk assessment or cybersecurity maturity self-assessment.

1.5 USING THIS DOCUMENT

This report introduces a four-phase approach to cyber risk management for port operators, which follows common principles of risk management[10] [11]. The approach is not intended to provide a comprehensive methodology for cyber risk management but rather provide actionable guidelines for managing cyber risk that **can be mapped to any framework or methodology the port operator is currently using or may wish to use**.

The first three phases are also mapped to the steps of the risk assessment methodology (minimum assessment requirements) articulated in the ISPS Code, Regulation 725/2004 and described in Annex I of Directive 2005/65. The fourth phase introduces a model for port operators to employ in performing cybersecurity maturity self-assessments for the selected security measures, identifying priorities for investing resources for improvement and/or building the programmatic foundations for organisational cybersecurity maturity. The four phases are:

- Phase 1: Identifying cyber-related assets and services (*ISPS Code Section 15.5.1: Identification and evaluation of important assets and infrastructure it is important to protect*)
- Phase 2: Identifying and evaluating cyber-related risks *(ISPS Code Section 15.5.2: Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures*, *ISPS Code Section 15.5.4: Identification of weaknesses, including human factors in the infrastructure, policies and procedures*)
- Phase 3: Identifying security measures (*ISPS Code Section 15.5.3: Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability*)
- Phase 4: Assessing cybersecurity maturity

Figure 1: Cyber risk management phases

Each of these four phases is reviewed in Chapters 2 – 5, respectively, with a specific emphasis on the following themes:

- Actionable **guidelines** to assist port operators in their efforts to perform each phase. These include specific guidance in how to effectively apply the various taxonomies presented in ENISA's Port Cybersecurity report of 2019[12].
- **Challenges** associated with the performance of activities as reported by port stakeholders who were interviewed/surveyed for this report.
- **Good practices** that can be readily adopted and customised by individual organisations and easily tailored and integrated into any risk assessment methodology utilised by port operators.
- A **mapping of the listed good practices for each phase with the respective challenges** they address.

[10] ISO 31000:2018, Risk management – Guidelines
[11] ISO 31010:2009 – Risk Management – Risk assessment techniques
[12] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

1.6 METHODOLOGICAL APPROACH

Figure 2: Methodology adopted for the study

Task 1 - Definition of the project scope and identification of experts: This first step consisted of establishing the scope of the project and selecting subject matter experts whose input and insights were considered for the development of the report.

Task 2 - Desktop research: This involved the collection of information from reports, white papers, and guidelines, as well as EU and (inter-)national regulations and industry-specific standards concerning cybersecurity risk management and relevant maturity models.

Task 3 - Questionnaire and series of interviews with selected subject matter experts: During this task interviews were conducted and an online survey was designed and published by ENISA to collect additional information. Specifically, **18** semi-structured interviews were performed with stakeholders representing **11 EU Member States** and **49** responses were collected from the survey, which collectively represented a wide cross-section of port industry stakeholders from 16 EU member states. Overall, inputs were collected from 20 port authorities, 17 terminal operators, 6 EU National Competent Authorities including EMSA, 17 shipping companies, 4 service providers and an EU research institute.

Task 4 - Analysis of collected material and report development: All inputs collected from desktop research efforts and collaboration with stakeholders were thoroughly analysed. Based on this analysis, the first draft of this report was developed.

Task 5 - Review and validation: The report was reviewed with and subsequently validated by ENISA's subject matter experts. Feedback was solicited and provided by experts throughout this process.

2. IDENTIFYING CYBER-RELATED ASSETS AND SERVICES

2.1 GUIDELINES FOR IDENTIFYING CYBER-RELATED ASSETS AND SERVICES

Phase one focuses on the identification of key IT and OT assets and the port services they support. In general, port operators should follow a service-based risk assessment in order to focus mainly on the aggregated business/operational impact of risks, However, port operators functioning at a more nascent stage of cybersecurity maturity will likely focus initial efforts on asset identification and enumeration.

The identification and evaluation of these assets, systems and services is not necessarily constrained to the organisation's own operational ecosystem. Ports represent complex ecosystems where assets and systems are increasingly integrated and interconnected, resulting in service-based interdependencies and voluminous data exchanges that occur every day.

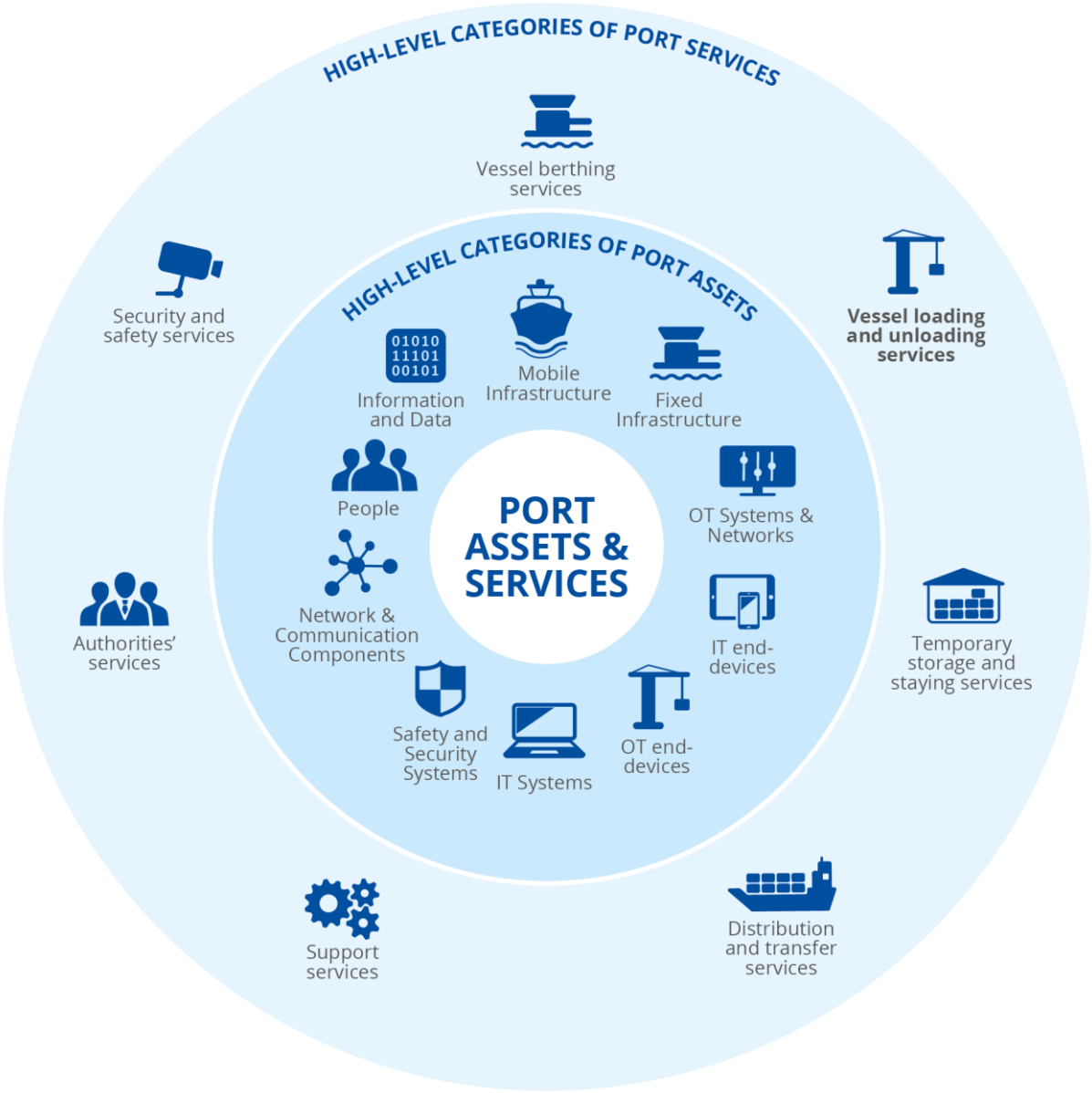
At the same time external third-party stakeholders (partners, vendors) frequently request or maintain continuous access to port IT/OT assets, systems, supporting infrastructure, and data, exponentially increasing the attack surface for potential malicious cyber threat actors. With all those touch points, especially those found in port community system enabled environments, vulnerabilities will inevitably arise. Within the context of this digital environment the port must be able to assess its ability to continue provisioning services in the event an asset, system or service is rendered unavailable as a result of a cyber incident, and also understand the extent to which rapid re-establishment of normal operation is possible.

Specific actions that port operators can perform include:

- Identify cyber-related assets and related services
- Develop indicators to assess cybersecurity incident impact on cyber-related assets and related services (e.g. number of users affected, economic impact, environmental impact, recovery time objectives etc.)
- Assess impact on the availability of cyber-related assets and related services
- Assess impact on the integrity of cyber-related assets and related services
- Assess impact on the confidentiality of cyber-related assets and related services
- Identify internal dependencies
- Identify external dependencies with third parties

ENISA's 2019 report on Port Cybersecurity identifies the main port services and infrastructure and presents a port asset taxonomy. Port operators can use the proposed taxonomies as the basis to identify their key cyber-related assets and services. The high-level categories of these assets and services are depicted in Figure 3, while the ENISA 2019 report provides a detailed description of each taxonomy.

Figure 3: High-level categories of port assets and services



2.2 RELATED CHALLENGES

- Difficulty in **identifying vulnerable IT and OT systems**. As different departments/divisions handle a variety of IT and OT equipment, identifying the vulnerable systems based on predefined criteria is challenging.
- Difficulty in **compiling and maintaining IT and OT systems risk registries.**
- Difficulty in **evaluating 3rd party-managed assets and services.**
- Difficulty **in attributing all assets, applications, systems and staff that relate to the provisioning of specific services.** This involves data creation, processing, transmission, exchange, and storage, which involves numerous stakeholders, both internally and externally. Increasing integration, technology refresh, evolution and integration create a range of challenges.
- Difficulty in handling **configuration management of OT systems.** Most OT systems providers do not offer access to extensive configuration management interfaces such

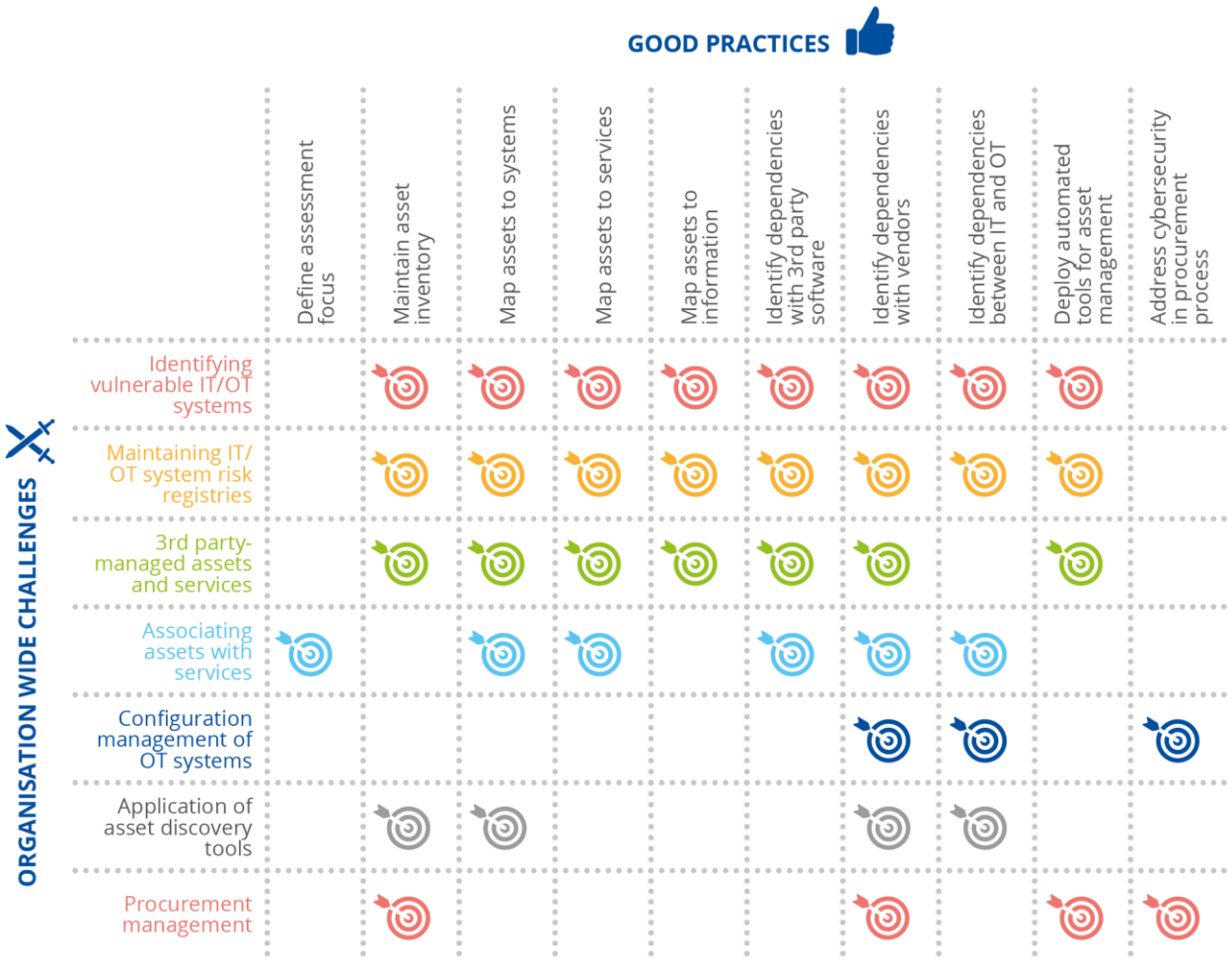
as user and system settings, which result in supply chain dependencies based more heavily on vendor support availability.

- Difficulty in **applying automated tools for identifying cyber-related assets**, since the deployment of such tools may inadvertently interfere with the normal functioning of critical OT assets, which may rely on legacy system/software or reside on segmented networks.
- Difficulty in managing the **procurement of software-enabled assets and stand-alone applications** due to local performance, compliance and/or certification requirements resulting in varying procurement mechanisms. This challenge is greater for large organisations with multiple business units, i.e. a company operating several port terminals around the globe.

2.3 RELATED GOOD PRACTICES

- Define the **assessment focus**. It is critical to define the specific focus of the assessment based on the unique characteristics of the port operator. An assessment can be asset-based or service-based, such as loading and unloading of containers, where several applications and assets are used to deliver specific services.
- Maintain an **asset inventory** for cyber-related assets.
- Assets should be **identified and registered** in the asset inventory **by the System they relate to.**
- Assets should be **identified and registered** in the asset inventory **by the Service they support.**
- Assets should be **identified and registered** in the asset inventory **by the Information they handle.**
- Dependencies should be **identified on the technical interface (and/or data exchange) requirements with third party software.**
- Dependencies should **be identified on the technical interface (and/or data exchange) requirements with vendors.**
- Dependencies should **be identified on the technical interface (and/or data exchange) requirements between IT and OT systems.**
- Deploy **automated tools for asset identification, logging and monitoring.**
- **Include the department/division responsible for cybersecurity in procurement contract review and implementation** in order to ensure cybersecurity is addressed.

Figure 4: Mapping of good practices against challenges in identifying and evaluating cyber-related assets and services



3. IDENTIFYING AND EVALUATING CYBER-RELATED RISKS

3.1 GUIDELINES FOR IDENTIFYING AND EVALUATING CYBER-RELATED RISKS

Phase two focuses on the identification and evaluation of cyber risks related to the assets and services identified in phase one. There exist a variety of methodologies and frameworks that offer detailed steps for how risk identification and evaluation should occur. For instance, the ISPS Code recognizes threat identification and vulnerability identification as essential and distinct activities in the performance of a port facility security assessment. Regardless of the methodology, framework or standard employed, results derived from this phase should include the identification of all relevant risks, which should be accompanied by an analysis of their likelihood and potential impact expressed in either a quantitative (e.g. score-based) or qualitative way.

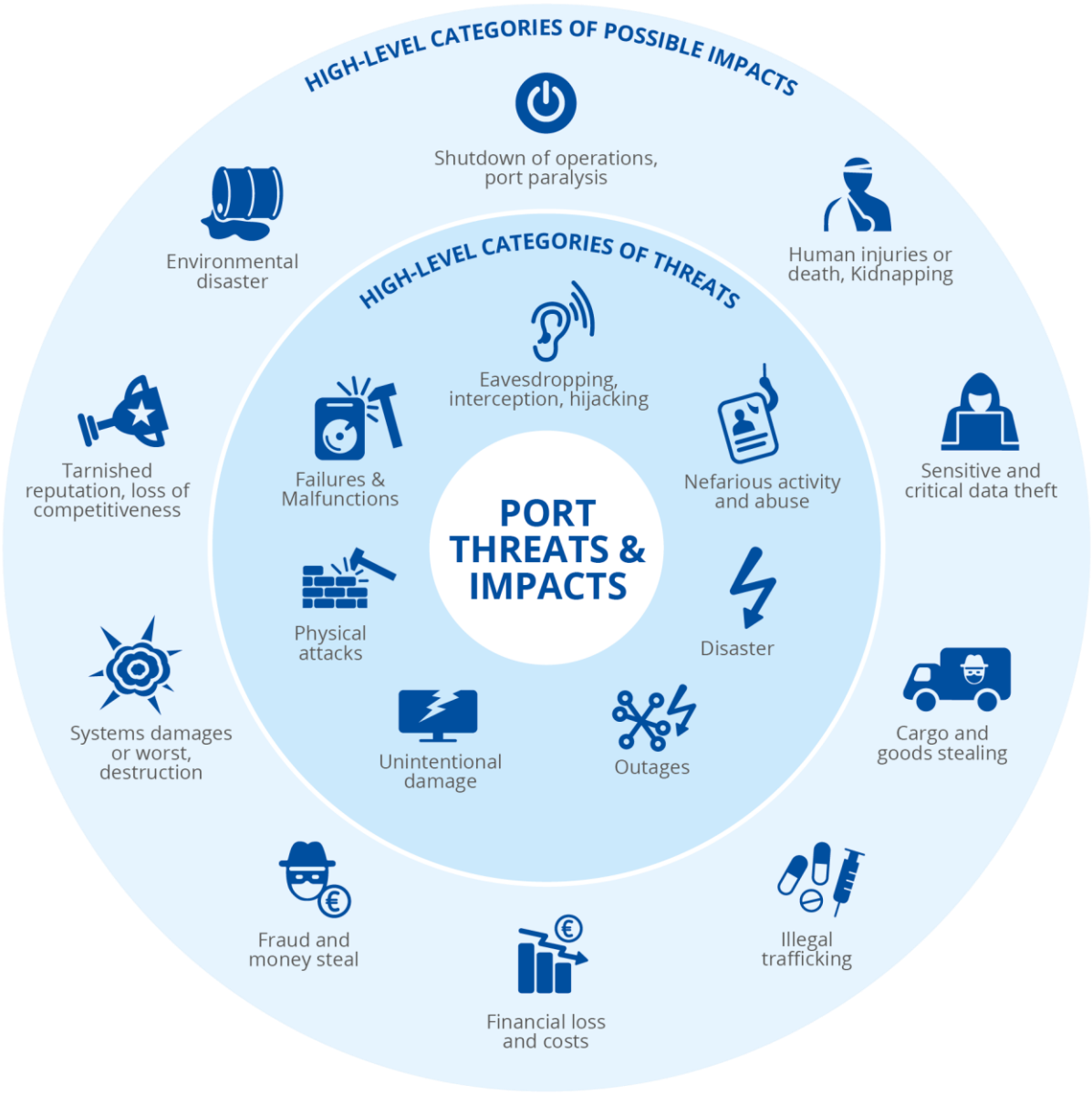
Specific actions that port operators can perform include:

- Contextualise the risk identification and evaluation process
- Identify cyber-related threats
- Identify vulnerabilities to assets and services
- Identify internal and external dependencies
- Assess the possible likelihood and impact of a cybersecurity incident
- Adopt a specific methodology for identifying and evaluating risks (e.g. scenario-based, empirical, data-driven, workshops/brainstorming sessions etc.)
- Develop indicators (qualitative or quantitative) to evaluate identified risks

Calculating the likelihood of occurrence of a cyber incident, along with identifying related vulnerabilities to assets, services, policies and procedures, is critical to establishing and prioritizing mitigation measures. It is commonly recognized by port stakeholders that although relatively minor threats may individually result in negligible impact to operations, a series of cascading minor threats, if left unaddressed, does harbour the potential to cause major disruption. Therefore, the identification of vulnerabilities should not be limited to assets and applications used in the organisation's ecosystem. Maintaining safe and secure operations also involves people handling the equipment and their adherence to defined policies, procedures and operational guidelines. Ultimately, any holistic vulnerability assessment should take the human element into consideration.

ENISA's 2019 report on Port Cybersecurity identifies the main threats to port assets and services and proposes a threat taxonomy and also lists the key possible impacts of cybersecurity incidents. Port operators can use the proposed taxonomies as the basis to identify their key cyber-related risks. The high-level categories of these threats and possible impacts are depicted in Figure 5. ENISA's 2019 report also provides a detailed description for each taxonomy.

Figure 5: High-level categories of threats and possible impacts of cybersecurity incidents



3.2 RELATED CHALLENGES

- **Cyber risk is not specifically identified** in currently utilized risk assessment methodologies.
- **Threats have been identified** for physical security and IT security**, but they are not combined for asymmetrical risk consideration.** Approved PSP/PFSPs reflect assessment inputs that have not been updated to accommodate (let alone acknowledge) the potential impact cyber threats pose.
- Difficulty in **calculating risk factors** (likelihood, impact of a cyber incident)
- Difficulty in **calculating aggregated risk**, as assets and services are increasingly interrelated within the digital port environment.
- Lack of **organisation-wide cyber awareness and commensurate cyber training,** which makes it difficult for staff to consistently identify threats and recognize potential

vulnerabilities of assets and services that may exist across the organisation's different departments/divisions.

- Lack of **recordkeeping regarding past incidents and subsequent response and recovery activities.**
- Lack of **information/intelligence regarding IT / OT systems' vulnerabilities,** actual and/or emergent.
- Lack of **available resources** (people, budget) **to carry out an effective risk assessment**, as they are perceived to be time-consuming and costly or require additional expenditures for obtaining information, such as automated vulnerability scanning tools etc.
- Difficulty in **defining cyber residual risk/risk acceptance thresholds**, based on the organisation's risk appetite.

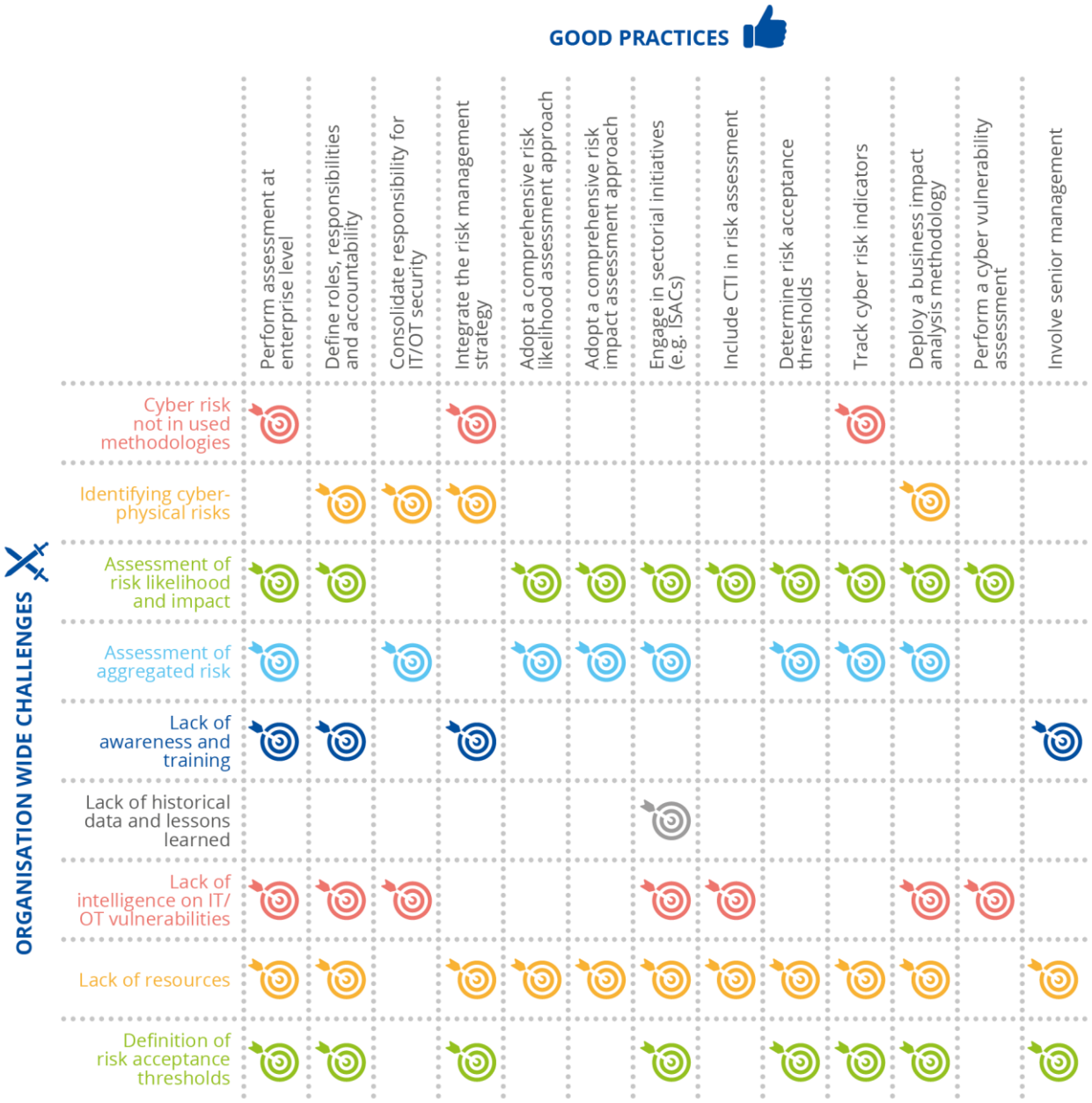
3.3 RELATED GOOD PRACTICES

- **Perform a cyber risk assessment at the enterprise level**. Engage representatives from all the departments/divisions in order to collect accurate information and solicit cross-functional insights.
- Clearly define **stakeholder responsibilities, authorities and risk ownership** for assets or services within each department/division/business unit.
- The security of IT and OT systems should be the **responsibility of the same department/division.**
- **Integrate cyber risk assessment** and management with existing risk assessment and management frameworks, such as the PSA/PFSA or PSP/PFSP and/or the organisation's **Enterprise Risk Management Strategy.**
- Adopt a **comprehensive and consistent approach to calculating the likelihood of occurrence for a cyber incident**, including factors such as threat actor motivation, their available resources, access to the port IT/OT infrastructure and target-specific knowledge.
- Adopt a **comprehensive and consistent approach to calculating the impact of a cyber incident**, in all business areas through a scenario-based approach that includes legal, reputational damage, health and safety, financial damage and business operations.
- Engage in sectorial initiatives, where organisations can liaise with each other to **identify common risks, share best practices and communicate in a secure and trusted environment**.
- Include **cyber threat intelligence (CTI)** inputs in the risk assessment methodology. CTI is a key capability that can provide critical insights into an organisation's potential risk exposure. In some cases, national competent authorities and/or commercial vendors can play a key role in the provision of such information to ports and port facilities.
- Develop a methodology to calculate **residual risk/risk acceptance determinations**. All risks in the risk registry should have an Inherent, Residual, and Target risk score. The inherent risk is the initial risk identified without any existing controls applied. If mitigation measures are in place, the risk can be given a residual risk score. If there are additional actions that can be taken to further mitigate that risk, it can be assigned a target risk score. Progress should be tracked and once the actions are completed the process can restart with the new risk score and the new inherent risk score.
- Develop a methodology to track **cyber risk indicators,** such as the number of infected systems per month, in order to identify trends and measure scope.
- Deploy a **business impact analysis methodology** which provides an assessment, using a **scoring mechanism**, against specific attributes, such as data **Confidentiality, Integrity, Availability, and operational safety and security**. Such a tool should also take into consideration systems' **criticality** and **sensitivity**. This can be **scenario-**

based, as it is easier for all stakeholders to understand how cyber threats can affect port operations.

- **Perform a cyber vulnerability assessment/penetration test.** This can help identify assets that may be unrecorded or not appropriately assessed and expose weaknesses in the port environment.
- **Involve senior management** in the process of defining residual risk/risk acceptance levels.

Figure 6: Mapping of good practices against challenges in identifying and evaluating cyber-related risks



4. IDENTIFYING SECURITY MEASURES

4.1 GUIDELINES FOR IDENTIFYING SECURITY MEASURES

Phase three focuses on the identification and prioritisation of security measures that should be implemented to reduce the identified risks to acceptable levels. Security measures should be adopted following a risk-based approach that directs budget, resources and technical capabilities towards the implementation of those security measures that will have the most substantial impact on the organisation's cyber risk posture. As such, this phase heavily relies on the evaluation of the identified risks.

Specific actions that port operators can perform include:

- Identify security measures to mitigate identified risks
- Assess the effectiveness and impact of the security measures in terms of how they influence the risk evaluation
- Assess resource requirements for the implementation of security measures
- Define a process for prioritising security measures

ENISA's 2019 report provides a comprehensive list of baseline security measures grouped in specific domains. When identifying security measures, port operators can reference the mapping in Table 1 to identify which security measures are most appropriate for protecting identified assets against acknowledged threats.

Table 1: Mapping of security measures to assets and threats

Domain	Security Measures	Assets	Threats
Security policy and organisation	PS-01: Information System Security Policy (ISSP)	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	PS-02: Security governance		
	PS-03: Share ISSP with all stakeholders		
	PS-04: Review ISSP annually		
Risk and Threats Management	PS-05: Risk-based approach	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	PS-06: Conduct and update risk analysis		
	PS-07: Security indicators and assessment methods		
	PS-08: Threat intelligence process		
Security and privacy by design	PS-09: Project methodology including security	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	PS-10: Privacy and compliance	People, Information and Data	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Unintentional damage, Physical attacks
	PS-11: Data classification	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
Asset inventory and management	PS-12: Asset inventory and management	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	PS-13: Policy for authorized devices/software	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Failures & Malfunctions
	PS-14: Asset monitoring	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions

Domain	Security Measures	Assets	Threats
Cyber Resilience (Business continuity and crisis management)	PS-15: Define objectives and strategic guidelines (BCP and DRP).	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	PS-16: Business continuity parameters (RTO, RPO, MTO etc.)		
	PS-17: Crisis management		
	PS-18: Training/exercises for recovery procedures		
Endpoints protection and lifecycle management	OP-01: Endpoint protection strategy	IT Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Physical attacks, Failures & Malfunctions
	OP-02: Device and software whitelisting		
	OP-03: Change management		
	OP-04: Return and disposal of end-devices		
Vulnerabilities management	OP-05: Vulnerability management process	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	OP-06: Intelligence processes for cybersecurity		
	OP-07: Collaboration of OT and IT departments		
Human Resource Security	OP-08: Professional references of key personnel	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Nefarious activity and abuse, Unintentional damage
	OP-09: Cybersecurity training		
	OP-10: Security awareness raising program		
Supply chain management	OP-11: Third-party access control	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	OP-12: Partnership with third parties		
Detection and incident response	OP-13: Define categories of incidents	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	OP-14: Policy and procedures for incident detection and response		

Domain	Security Measures	Assets	Threats
	OP-15: Improve and update procedures		
	OP-16: Security Operations Centre (SOC)		
	OP-17: Define alerting procedures and communication plan		
	OP-18: Incident reporting and continuous improvement		
Control and auditing	OP-19: Cybersecurity audits	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Physical attacks, Failures & Malfunctions
	OP-20: Periodic reviews	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Physical attacks, Failures & Malfunctions
IT and OT physical protection	OP-21: Physical protection for safety	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	OP-22: Maintenance operations traceability		
Network security	TP-01: Network segmentation	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse
	TP-02: Regular network scans		
	TP-03: Perimetric security		
Access control	TP-04: Centralised tools for IAM	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage
	TP-05: IAM strategy		
	TP-06: Restrict generic accounts		
	TP-07: Password complexity policies/rules		
	TP-08: Multi-factor authentication		
	TP-09: Physical/remote access control	Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Physical attacks
	TP-10: Accounts and access right reviews	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, People, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Physical attacks

Domain	Security Measures	Assets	Threats
Administration and Configuration Management	TP-11: Installation and configuration policy	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage
	TP-12: Administrators accounts		
	TP-13: Privilege Account Management		
	TP-14: Dedicated administration networks		
Threat management	TP-15: Anti-malware, anti-spam and anti-virus	IT Systems, Safety and Security Systems, IT end-devices	Nefarious activity and abuse
Cloud security	TP-16: Cloud security assessment method	IT Systems	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	TP-17: Security / availability in cloud SLAs		
	TP-18: Cloud options for detection/response		
Machine-to-machine security	TP-19: Secure M2M exchanges	OT Systems & Networks, OT end-devices, IT Systems, Information and Data	Eavesdropping, interception, hijacking, Nefarious activity and abuse
	TP-20: Secure communication protocols		
Data protection	TP-21: Cryptography	Information and Data	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Unintentional damage, Failures & Malfunctions
	TP-22: Anonymise / secure personal data		
Update management	TP-23: Define update management process	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Failures & Malfunctions
	TP-24: Software/firmware authenticity		
	TP-25: Verify the source of updates		
Detection and monitoring	TP-26: Monitor availability of the port systems and devices	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
	TP-27: Logging system		
	TP-28: Log correlating and analysis systems		

Domain	Security Measures	Assets	Threats
Industrial control systems security	TP-29: OT systems in security measures	OT Systems & Networks, OT end-devices, Information and Data	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Failures & Malfunctions
	TP-30: Network segmentation between IT/OT	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse
	TP-31: Specific security measures for IoT	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Eavesdropping, interception, hijacking, Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions
Backup and restore	TP-32: Set up backups and ensure they are regularly maintained and tested	OT Systems & Networks, OT end-devices, IT Systems, Safety and Security Systems, Information and Data, Network & Communication Components, IT end-devices	Nefarious activity and abuse, Disaster, Outages, Unintentional damage, Physical attacks, Failures & Malfunctions

4.2 RELATED CHALLENGES

- Difficulty in **assessing the effectiveness of mitigation measures**
- **Lack of available internal resources** (people, time, budget) for the identification, adoption, implementation and review of suitable mitigation measures.
- **Difficulty in sharing established security measures**, procedures and policies, both **internally and externally**, with third party stakeholders, which impedes the development of a common approach to driving port community resilience.
- Difficulty in **identifying and selecting security measures based on business continuity requirements.** Most port stakeholders are currently focused on implementing security measures in response to cyber incidents instead of adopting proactive security measures.
- The perception that any attempt to **protect the entire organisation against cyber threats may exhaust organisational resources** (time consuming, costly, large number of dedicated staff, etc.).

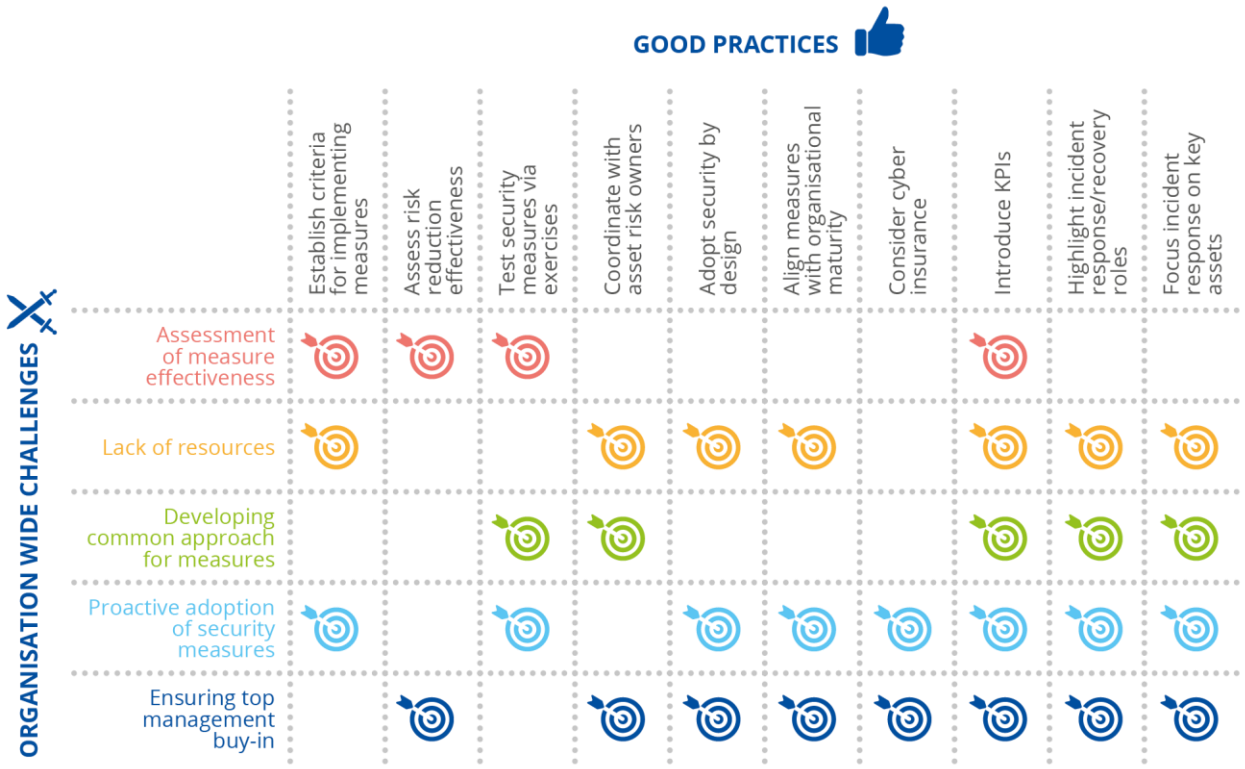
4.3 RELATED GOOD PRACTICES

- **Implement security measures based on predefined criteria,** applicable to the entire organisation, such as those that drive **cost reduction, deliver risk reduction and/or reduce the impact of a cyber incident.**
- **Assess all security measures for risk reduction effectiveness** by implementing a scoring methodology.
- **Test security measures during cyber drills/exercises**, or security drills/exercises that include detailed cyber elements, both **internally and externally** with port stakeholders.
- **Coordinate the identification, adoption and implementation of security measures with the asset risk owner**.
- Adopt a **'security-by-design**' approach in all procurement activities. Taking cybersecurity into consideration in the conceptualisation phase of a project minimises the need for additional allocation of resources during the operational cycle of the asset/service.
- - For **less mature organisations** focus on identifying and implementing security measures that offer **detection, response and recovery capabilities** in the event of a cyber incident.

  - For **mature organisations** focus on identifying and implementing security measures that **protect the organisation's most critical assets/services.**
- Consider **cyber insurance** as a risk reduction mitigation measure. Cyber insurance can contribute to the organisation's resilience by reducing risk of financial loss and can also help to mobilize resources (e.g. funding, expertise) quickly in response to a cyber incident.
- Introduce **cyber specific metrics, or Key Performance Indicators (KPIs)**, such as monitoring the availability of IT and OT assets and related services, awareness levels of staff, number of critical security incidents etc. These should be periodically reported to and reviewed by senior management.
- Highlight the **role of individuals as the first line of defence, response and recovery**. Training plays a prominent role in raising awareness and developing capacity in responding to cyber incidents.
- For effective incident response, prioritise **response capabilities to focus on key business-critical assets / services / departments / divisions / business units,** along with the organisations they are connected to in order to contain a potential cyber incident.

Figure 7 maps the relevant challenges and good practices.

Figure 7: Mapping of good practices against challenges in selecting and prioritising mitigation measures



5. ASSESSING CYBERSECURITY MATURITY

5.1 INTRODUCTION

Phase four goes beyond the adoption of baseline security measures to identify areas where port operators can improve their cybersecurity maturity. The process of cybersecurity maturity self-assessment can support organisations in their efforts to understand where they currently stand in terms of maturity in security domains – or individual security measures – of interest and plan their organisational progression accordingly.

Identifying where organisations need to improve their cybersecurity practices informs the prioritisation and allocation of limited resources that will result in the most effective outcome. This chapter lists the security measures proposed in the 2019 ENISA report and introduces maturity levels that port operators can select to help prioritise security measures and conduct a self-assessment for the purpose of determining their current maturity level. Results from this effort will guide stakeholders in their selection of security measures and better understand the specific actions they should undertake in order to improve their organisational cybersecurity capabilities, and thus achieve higher maturity levels.

A maturity self-assessment model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. This provides a benchmark against which an organisation can evaluate the current level of capability exhibited by the day-to-day implementation of its controls, practices, processes, tools, and personnel, and supports stakeholders in their effort to set goals and priorities for continuous improvement

A maturity model approach relies on the fact that effective cyber risk management cannot be achieved through a “checklist mentality”, since cyber threats represent a persistent, constantly evolving risk to port operations. Achieving and sustaining organisational cyber resiliency requires effective cyber risk assessment and management at an organisational level.

The first step to effective cyber resilience is the establishment of an organisation-wide cybersecurity capability baseline that is commensurate with the nature and scale of the cyber risks associated with its operations and supporting supply chain. To establish a realistic baseline requires that port organisations gain situational awareness of their current cybersecurity capabilities and identify the cybersecurity capability gaps that may exist.

The next step includes the “institutionalisation” of the organisation’s existing cybersecurity capability posture, throughout the various business assets, services, and processes. This is achieved through structured and well-defined recurring activities focused on maintaining an increased cyber risk awareness, revised risk-based behaviours, and appropriate resource allocation (people, processes, tools and funding).

The approach proposed here is based on the introduction of maturity levels of implementation for the security measures proposed in the 2019 ENISA report on Port Cybersecurity. Each maturity level includes a description of what the organisation needs to put in place in order to achieve the respective level.

5.2 RELATED CHALLENGES

- **Lack of communication** between the departments responsible for physical security and cybersecurity. Poor (or lack of) effective communication is frequently exacerbated by the fact that in the majority of cases personnel responsible for physical security risk management fail to communicate with and/or involve cybersecurity or IT experts in security planning, coordination, and preparation activities.[13]
- **The IT department is tasked to assume the responsibility for cybersecurity without appropriate training** or internal coordination with other departments.
- **IT and OT systems are the responsibility of different working groups or divisions**, and, therefore, fall under different organisational authorities (usually IT and Technical). Thus, efforts to develop a holistic cybersecurity strategy that address both IT and OT systems are often uncoordinated and inconsistently resourced.
- Cybersecurity maturity varies among different groups or operating divisions across the organisation, including senior management and board of directors. This is usually a result of a **lack of organisation-wide cyber awareness and related cyber training,** including tailored training for executives**.**
- **Lack of available resources** (people, processes, tools, budget, time) to fully organize, develop, conduct and regularly update the organisation's baseline cyber risk assessment.
- **Difficulty in staffing**. This is exacerbated by the shortage of cybersecurity experts currently available in the global market.
- **Difficulty in assigning internal roles.** This is worsened by the difficulty among key stakeholders in fully apprehending the nature of the cyber threat.
- **Difficulty in managing internal change.** Organisations finding it difficult to encompass and comprehend changes made to existing policies and procedures regarding cybersecurity.
- **Difficulty in third-party management**. Larger organisations with several business units and external partners are finding it difficult to implement a consistent cyber risk management approach across their organisation.
- **Variety of cyber risk assessment standards/frameworks**. The large number of standards regarding IT security, cybersecurity or risk assessment is causing confusion to port stakeholders, making the selection and implementation of the appropriate standard or framework challenging for organisations with limited resources or low cyber maturity.
- **Fragmentation and distribution of governance of ports operators**. Ports are characterized by a very fragmented and distributed governance especially in the private sector. Frequently, organisations or entities responsible for part/full of operations at ports comprise multiple stakeholders, and cybersecurity responsibilities are unclear and complex to implement.

5.3 RELATED GOOD PRACTICES

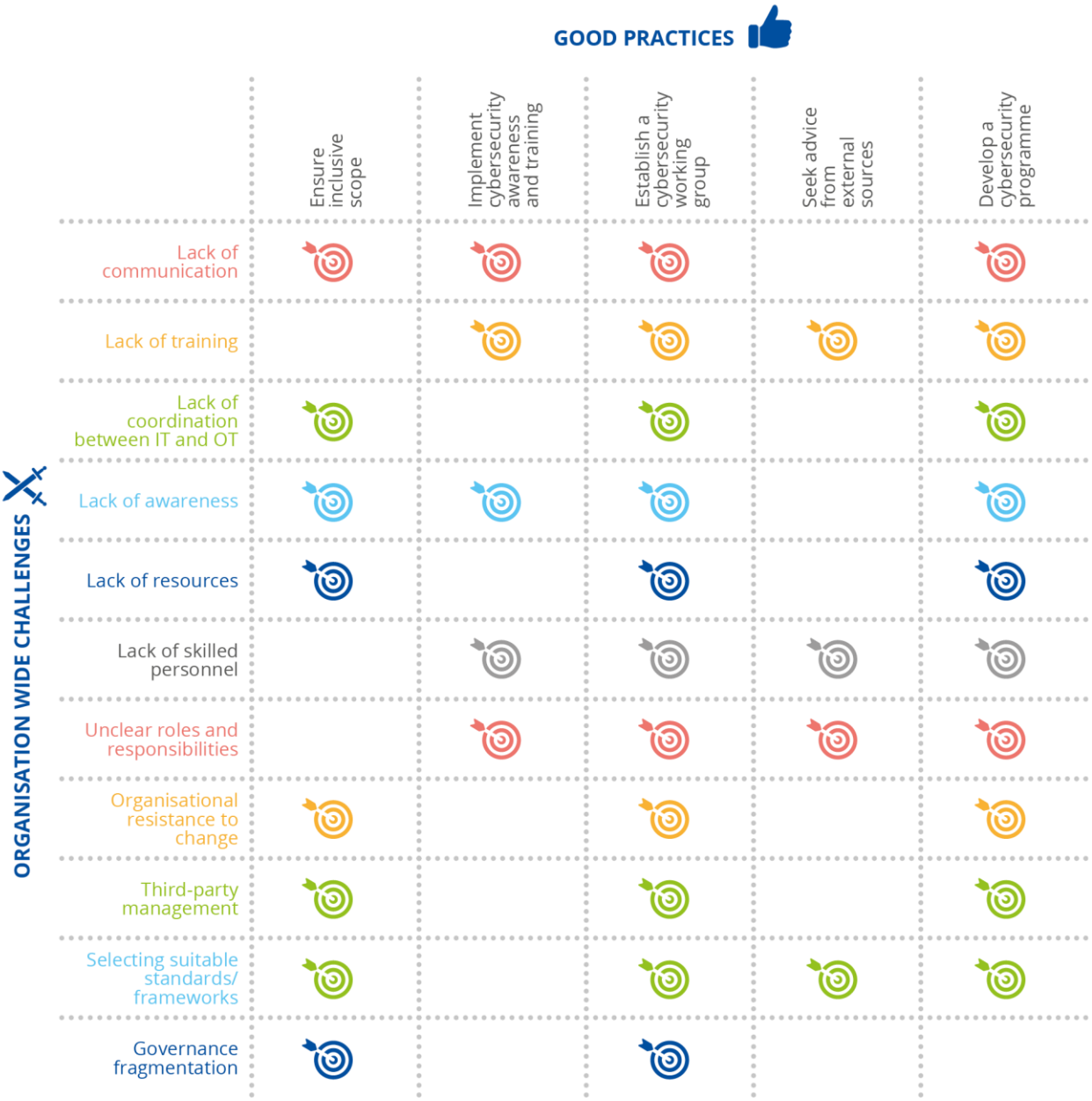
- **Ensure the cyber risk assessment includes all aspects of the scoped environment.** As cybersecurity is not only an IT issue, linking it to all plans, policies, resources and capabilities are included to ensure a more accurate determination of the current cybersecurity state and the implementation of cyber risk assessment good practices.
- **Implement cybersecurity awareness and technical training programmes**. Awareness training represents a fundamental capability in addressing several of the aforementioned challenges. Standardized training ensures consistency in establishing

[13] A key common factor behind all these challenges is how cybersecurity is positioned in the maritime sector. Cyber security is still mainly viewed as an IT problem. Isolating cybersecurity in the IT department and lack of appropriate reporting lines for cyber risk within the organisation results in limitations in terms of responsibility, competences, approach, resources, budget, etc.

minimum cybersecurity awareness across all staff irrespective of their functional activities. Also, develop and deploy specific content that is relevant for the organisation's operating environment and to educate staff specifically on how to safely and securely access and use corporate, software-enabled, assets and equipment.

- **Formally organize a cybersecurity working group**. Staff with key leadership and/or representatives from each of the organisation's operational areas and/or divisions. All functions of the organisation should be represented, and individuals should be assigned specific responsibilities. Establish a regular schedule, preferably monthly, and grant appropriate authorities to the group to support cyber risk management activities. The working group size will vary by organisation.
- **Seek advice from external sources**, such as contracting governments, national/international competent authorities or private companies. Using external assistance to secure guidance on how best to implement and sustain cyber risk assessment standards/ frameworks can help an organisation avoid repeating mistakes.
- **Develop a cybersecurity programme**. This should include a cyber risk management strategy that is supported by documented plans, policies, procedures, and internal guidelines informed by referenced standards. This should identify and define the cybersecurity working group, resource allocations, training, performance objectives, budgets and the various cyber risk management activities that are performed to meet defined cybersecurity objectives.

Figure 8: Mapping of good practices against challenges in addressing cybersecurity maturity



5.4 PORT CYBERSECURITY MATURITY LEVELS

The proposed approach is structured to (1) assess an organisation's cybersecurity capabilities over three maturity levels and (2) follow a dual progression approach that characterizes both capability progression and institutionalisation is adopted:

- *Capability progression* measures the degree to which the organisation has implemented cybersecurity capabilities (people, processes, tools, and funding).

- *Institutionalisation* measures how deeply entrenched specific activities, controls, processes, and procedures are within and across the organisation. The more ingrained these are, the more likely the organisation will maintain them consistently during and after an incident.

Additionally, the three maturity levels of the proposed approach are defined in Table 2.

Table 2: Maturity level definitions

Maturity Level	Description
1 (Basic)	This level corresponds to the minimum-security measures that are implemented to achieve a security objective. The organisation performs baseline activities and/or capabilities, even in an ad hoc manner.
2 (Intermediate)	This level corresponds to more sustained capabilities that align with identified standards and best practices. The organisation implements, manages, monitors, and measures capabilities against defined objectives and operational applicability. Documentation (i.e. plans and policies) guides the application and utilisation of resources for specific and/or coordinated activities.
3 (Optimal)	This level corresponds to activities and/or capabilities that are planned, tested, policy-informed, and repeatable; subject to regular oversight and reviews to confirm effectiveness; and improve the implementation of security measures, taking into account disciplined changes, tests, and exercises. The organisation regularly measures capabilities to support continuous improvement efforts to attain and sustain defined performance objectives.

Section 5.5 provides **examples of the proposed maturity levels** for the security measures defined in the ENISA 2019 report. Port operators can use the information therein as follows:

1. Following their own implementation of the previous risk assessment/management phases, port operators can identify a list of security measures that are most relevant to them.
2. Port operators can then review the policies, practices and technical measures throughout the tables in section 5.5. For each security measure, the respective maturity level indicates **examples** or **evidence** that the measure is implemented at a specific maturity level.
3. Port operators should carefully consider the evidence/examples to ensure relevance to their operational environment and appropriateness to capabilities. For example, operators such as customs are not required to consider examples related to PSPs/PFSPs requirements, while a port authority may have a Port Security Officer but not a Port Facility Security Officer. Similarly, the examples/evidence provided should be tailored by the port operator to match their organisation's unique characteristics regarding cyber risk management (e.g. terminology, information security framework etc.).
4. Port operators should assess their current maturity level in terms of implementing the selected security measures by determining how their current practices map to the maturity levels of the provided examples/evidence. It's important to note that in many cases a port operator may select one or more security measures that may result in an organizational cybersecurity posture that reflects variable maturity levels.
5. Port operators can identify priorities for improvement depending on specific needs, as well as determine the viability of and benefits derived from actions that can be easily and quickly implemented.

5.5 MATURITY LEVELS FOR PORT CYBERSECURITY MEASURES

5.5.1 Policies

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Security policy and organisation			
PS-01: Write and implement an information systems security policy (ISSP), which describes all organisational and technical means and procedures, including topics related to the OT environment. This ISSP must be approved by the port's top management team to guarantee the high-level endorsement of the policy. Key elements of the ISSP can be integrated in the Port Facility Security Plan required by the ISPS Code.	• The organisation has drafted one or more information system security policies (ISSPs) that provide technical guidance and supporting procedures to stakeholders in protecting information technology and operational technology environments. • The ISSPs include cybersecurity considerations. • The organisation's designated Port Facility Security Officer is familiar with the ISSPs. • The organisation has updated its PSP/PFSP to include ISSPs.	• The organisation has formally codified its ISSPs in an overarching plan that provides tailored guidance to stakeholders regarding the organisation's unique IT/OT environment. • Top management have reviewed and approved the organisation's ISSPs. • The updated PSP/PFSP includes a cybersecurity appendix (or annex) that includes all relevant ISSPs addressing cybersecurity considerations.	• The organisation regularly reviews its ISSPs to ensure that policies and procedures accord with defined objectives. • The organisation includes ISSP elements within quarterly drills and annual exercises to align security activities with IT/OT operating environments. • The organisation shares its ISSPs with key stakeholders across the organisation.
PS-02: Enforce security governance of both IT and OT environments through the ISSP by describing the roles and responsibilities of each stakeholder (Port Authority, terminal operators, service providers, suppliers, etc.	• The organisation has identified and defined roles and responsibilities for stakeholders responsible for supporting security activities across all IT and OT operating environments. • The organisation has established stakeholder roles and responsibilities supporting security activities and identified them within one or more ISSPs. • Stakeholder roles and responsibilities supporting security activities distinguish between internal and external stakeholder engagement.	• The organisation has established and documented within its ISSPs a senior leadership role (or roles) that defines responsibility for managing cyber risk across all areas of the organisation, including IT and OT environments. • The organisation has defined and documented executive and senior leadership roles and responsibilities in order to identify the individuals responsible for managing and mitigating cyber risk factors when the organisation suffers a cyber-incident. • The organisation has clearly defined the Managing Director's role and responsibilities for cybersecurity oversight, post-incident response, and crisis communications after a cyber-incident.	• The organisation reviews stakeholder roles and responsibilities at least annually to ensure that proper oversight of all IT and OT environments.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
PS-03: Share the ISSP with all stakeholders involved in port operations, or, if more relevant a light version underlying each party responsibilities towards cybersecurity at port level.	• The organisation shares its ISSP, or relevant information within the ISSP, with all stakeholders involved in port operations. • The organisation's ISSP articulates each party's cybersecurity responsibilities at the port level.	• The organisation shares its ISSP, or relevant ISSP elements, with all stakeholders involved in port operations consistent with a documented procedure that identifies with whom to share the document. • The ISSP's documentation sharing procedure(s) includes notification procedures.	• The organisation regularly reviews ISSP documentation to revalidate cybersecurity responsibilities of named stakeholders involved in operations at the port level.
PS-04: Review annually the ISSP by considering the results of cyber security tests and risk analysis to tackle new threats and risks.	• The organisation's leadership reviews ISSP or similar security documentation, audit results, and test findings to identify areas requiring updating.	• The organisation has a documented process that facilitates annual reviews of cybersecurity audit, test, and/or evaluation results against existing ISSP or similar documentation cybersecurity to identify areas requiring updating.	• The effectiveness of the ISSP review process is assessed to identify continuous improvement objectives (e.g. additional sources of input for the annual ISSP review).
Risk and threats management			
PS-05: Adopt a risk-based approach to build the port cybersecurity strategy and set up a continuous improvement process to ensure that the risks identified are under control and that new risks are properly identified in a timely manner. Ensure identified cyber risks are considered in safety and security plans to align cybersecurity with physical security and safety (in particular, through the Port Facility Security Assessment required by the ISPS Code).	• Consistent with the IMO's ISPS Code requirements, the organisation has conducted a port facility security assessment that includes cybersecurity risks. • The organisation evaluates existing health and safety, security, and incident response plans to ensure alignment with cyber risk management best practices. • The organisation maintains, references, and communicates established best practices to support cyber risk management activities in both administrative and operational environments. • The organisation has evaluated cyber risk factors for their potential to impact the organisation's regulatory compliance.	• The organisation has identified cyber risks in facility security assessments and considered cyber risks in safety and security plans in order to align cybersecurity with physical security and safety. • Cyber risk management policies and procedures are documented for all IT/OT environments and align with the organisation's defined performance objectives, which include resilience requirements to support delivery of critical services. • To verify effectiveness and operational readiness, the organisation performs regular internal audits and/or inspections against defined policies, including regulatory regimes that include documented cyber risk. Management policies and/or procedures.	• As part of the organisation's continuous improvement process, updated cyber risk criteria are accessible to stakeholders for use in re-validating cyber risk impacts to critical assets, systems, and/or services; re-affirming organisational cyber risk tolerances, such as risk mitigation, acceptance, or transfer; and re-confirming cyber incident response elements. • The organisation reviews its cyber risk management practices, procedures, directives, and/or or related activities at least annually to ensure adherence to documented requirements and defined performance objectives in order to ensure adherence to established standards. Lessons learned are documented.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
PS-06: Conduct and regularly update risk analysis to identify risk and threats related to the port ecosystem. In particular, risk analysis must be conducted for new projects (SmartPort initiatives such as Big Data, IoT, blockchain, etc.).	• The organisation performs regular audits of its Port Facility Security Plan consistent with the requirements of the IMO's ISPS Code. • PFSP and PSP audits include analysis of cyber risk factors that can impact both the organisation specifically and the broader port community within which the organisation functions.	• The organisation conducts risk assessments for all projects and initiatives, such as those involving the adoption of new technologies and systems (e.g., Big Data, Internet-of-Things enabled systems, Blockchain, etc.), in order to identify potential cyber vulnerabilities. • The organisation performs threat assessments to inform recurring risk assessment activities.	• The organisation regularly reviews and updates to reflect the current cyber threat environment its cyber risk management strategy, which includes cyber risk tolerances for services, systems, and assets supporting administrative and operational areas and risk response options. • The organisation has identified cyber risk factors (including threats) for IT and OT systems that may impact complex infrastructure and/or other critical assets or control systems whereby an incident may threaten health and safety of staff and/or jeopardize the surrounding port community.
PS-07: Set up security indicators and assessment methods to evaluate the compliance of the port systems and processes to the ISSP and risk management performance, by involving several stakeholders when relevant.	• The organisation has a mechanism or process that facilitates the collection of cybersecurity threat information from internal and/or external sources. • The organisation has performed a vulnerability assessment of its IT/OT operating environment.	• Threats and vulnerabilities are analysed to determine relevance to the organisation's operating environment, including its compliance posture. • The organisation has a process in place to facilitate the analysis, prioritization and mitigation of threats and cybersecurity gaps identified in a Vulnerability Assessment. • The organisation has rules and supporting procedures (within ISSPs) that guide the sharing of newly discovered threat and/or vulnerability information among relevant internal and external stakeholders.	• As part of the organisation's continuous improvement process, updated cyber risk criteria are accessible to stakeholders for use in re-validating cyber risk impacts to critical assets, systems, and/or services; re-affirming organisational cyber risk tolerances, such as risk mitigation, acceptance, or transfer; and re-confirming cyber incident response elements. • Documented cyber threat monitoring and response activities inform, leverage and trigger pre-defined security and operational states (i.e. Maritime Security Level changes). • The organisation's documented threat and vulnerability management plans, policies, procedures are regularly reviewed in ensure conformance with defined goals and referenced standards.
PS-08: Set up a threat intelligence process to watch continuously for vulnerabilities, identify new risks and threats and deploy actions to mitigate them.	• The organisation has a mechanism or process that facilitates the collection of cybersecurity threat information from internal and/or external sources. • The organisation has invested in tools and/or methods to support the identification of vulnerabilities in assets and/or detect malicious code in assets (including mobile assets). • The organisation tracks the status of unresolved threats and vulnerabilities and informs system/asset owners of that status.	• The organisation has developed documented policies that guide vulnerability analysis and resolution activities. • The organisation has a process to facilitate the analysis, prioritization, and mitigation of cybersecurity gaps. • The organisation has allocated adequate and risk-appropriate resources (people, tools, and funding) to support threat and vulnerability management activities.	• Documented cyber threat monitoring and response activities inform, leverage, and trigger pre-defined security and operational states, such as changes to the Security Level. • The organisation's management regularly reviews documented threat and vulnerability management activities for effectiveness. •

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Security and privacy by design			
PS-09: Develop a project methodology including security assessments and checkpoints, including for agile projects (risk analysis, architecture security review, security tests, security approval, etc.) for new and existing projects, considering the criticality and exposure of the system. More specifically, strongly include cybersecurity issues in SmartPort projects from the design stage to implementation.	• For all new and ongoing projects and initiatives, the organisation employs a risk assessment methodology that includes an overall risk review, an architecture security review, test and acceptance procedures, and a formal approval procedure. • The organisation has a current cybersecurity architecture that can be referenced in a documented security policy to manage recurring risk analysis.	• The organisation regularly performs cyber risk assessments of critical IT/OT systems and includes an analysis of dependent operations in SmartPort environments. • The organisation's network architecture informs cyber risk assessment activities addressing all critical IT and OT system environments.	• To support ongoing cyber risk management activities, the organisation regularly reviews and updates its risk register, which includes all risks identified through cybersecurity assessments for administrative and operational environments.
PS-10: Address privacy related issues based on applicable local and international regulations, such as the General Data Protection Regulation (GDPR).	• The organisation adheres to all local, national, and international regulations (e.g., GDPR), where applicable.	• The organisation has performed a Data Protection Impact Assessment (DPIA), where appropriate. • The organisation has established documented data protection policies, procedures, and processes, and security controls. • The organisation has formally established the role and responsibilities of a Data Protection Officer (DPO).	• The privacy assessment processes are reviewed periodically for effectiveness and suitability.
PS-11: Launch a data classification project to identify critical data for port operations as well as personal data and to protect them accordingly and to map the data flows, especially for personal data and operational data related to vessel, dangerous goods and cargo.	• The organisation classifies data critical to port operations. • The organisation classifies personal data to ensure privacy protections. • The organisation maps data flows	• The organisation documents data classification criteria in policies and/or procedures. • The organisation has mapped and documented data flows for critical IT/OT systems. • The organisation has documented data flows for all ship-shore interfaces (passenger list exchanges, Notice of Arrivals, dangerous goods and cargo, etc.).	• The organisation has documented all policies designed to specifically protect sensitive information, such as information defined by privacy regulations and commercial confidential, or third-party-sensitive-but-unclassified information. • The organisation reviews and re-validates data flow maps.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Asset inventory and management			
PS-12: Use centralized tools for asset inventory and management and ensure that you keep them up-to-date (applications, software platforms, networks, network components, servers, physical devices, OT systems, administration components, etc.)	• The organisation maintains an inventory of IT assets, including servers, related software applications, and, where applicable, software that supports operating systems of operational activities. • The organisation maintains an inventory of all OT systems, including, where applicable, software operating systems and related applications.	• The organisation has a process or procedure that facilitates management oversight of asset inventorying and change management activities. • The organisation has a process that facilitates efforts to maintain the inventory of all inter-connected assets as current.	• To ensure adherence to documented performance objectives, the organisation has a process that facilitates the regular monitoring of asset inventorying and change management activities.
PS-13: Define a policy regarding authorized devices and software to ensure than only reliable components are introduced to the port network.	• The organisation has a documented policy establishing authorization procedures for devices and software prior to deployment on any network. • The organisation tests new or modified IT, OT, and communication assets prior to deployment in the organisation's live operating environment. (Same as OP-03)	• The organisation documents all updates and changes to IT, OT, or communication systems following testing and prior to implementation. (Same as OP-03)	• The effectiveness of the policy regarding authorized devices and software is reviewed periodically.
PS-14: Use centralized tools to monitor the different assets by adapting them according the specificities and the associated risks (e.g. passive monitoring for OT systems) and detect unauthorized assets.	• The organisation monitors critical IT/OT assets for irregular activity.	• The organisation employs and configures endpoint monitoring tools to support organisation-specific requirements for monitoring critical IT/OT assets for unauthorized access. • The organisation has a documented policy that provides guidance regarding endpoint monitoring, alerting, and response activities.	• The organisation regularly reviews endpoint monitoring activities for effectiveness.
Cyber resilience (Business continuity and crisis management)			
PS-15: Ensure cyber resilience of port systems by defining objectives and strategic guidelines regarding business continuity and recovery management and set up associated key services and processes (Business Continuity Plan and Disaster Recovery Plan).	• The organisation has defined business continuity and disaster recovery objectives for port systems.	• The organisation has documented Business Continuity and Disaster Recovery Plans. • The organisation has identified and documented stakeholder roles and responsibilities within Business Continuity and Disaster Recovery Plans. • The organisation has identified and prioritized critical IT/OT systems are identified and prioritized within the Business Continuity and Disaster Recovery Plans.	• The organisation reviews its Business Continuity and Disaster Recovery Plans annually.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
PS-16: Define important parameters for port's business continuity, such as a recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).	• The organisation has identified all IT/OT systems that support critical port services.	• The organisation has established Key Recovery Time Objectives (RTOs) within the Business Continuity and Disaster Recovery Plans. • The organisation has established Key Recovery Time Objectives (RTOs) within the Business Continuity and Disaster Recovery Plans. • The organisation has established Key Recovery Point Objectives (RPOs) within the Business Continuity and Disaster Recovery Plans. • The organisation has established Minimum Business Continuity Objectives (MBCOs) within the Business Continuity and Disaster Recovery Plans.	• The organisation regularly reviews and re-validates recovery parameters within Business Continuity and Disaster Recovery Plans. • The organisation tests recovery parameters in drills and exercises.
PS-17: Define a crisis management organisation by formalizing a specific policy and by setting up the associated crisis management process, including all the port stakeholders.	• The organisation has identified resources to support crisis management activities.	• The organisation has a documented Crisis Management Plan and supporting policies and procedures that detail the organisational structure of a crisis response team and its functions. • The organisation has identified and assigned individuals roles and responsibilities to support the crisis response team.	• Agreements have been established with other port organisations that define communication protocols, information sharing procedures, resourcing capabilities, and processes to facilitate mutual aid in the event of a crisis.
PS-18: Ensure the efficiency of recovery procedures by setting up annual training exercises, making sure that all critical port stakeholders (local authorities, Port Authorities, terminal operators, service providers, etc.) are involved as much as possible, and by formalizing post-exercise reports.	• The organisation participates in drills and exercises that test crisis response activities involving multiple organisations.	• The organisation participates in the drafting of post-exercise reports that detail all findings and lessons learned. • The organisation disseminates post-exercise reports all training event participants.	• The organisation incorporates lessons learned derived from multi-organisational drills and exercises into the continuous improvement process. • The organisation updates Incident Response, Security, Business Continuity, and Disaster Recovery Plans using lessons learned.

5.5.2 Organisational practices

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Endpoints protection and lifecycle management			
OP-01: Define an endpoint protection strategy to monitor port end-devices and to enforce their security by implementing security tools and mechanisms such as antivirus, encryption, mobile device management (MDM) and hardening (disabling of unnecessary services, especially by securing USB ports in all port systems).	• The organisation employs endpoint protection to monitor port-end devices. • The organisation employs antivirus protection. • The organisation employs encryption. • The organisation performs mobile device management. • The organisation secures its USB ports.	• The organisation has a documented endpoint protection strategy that includes all networked environments.	• The organisation periodically reviews its endpoint protection strategy to ensure effectiveness. • The organisation's endpoint protection strategy aligns endpoint protection measures with security tools and mechanisms, such as antivirus, encryption, mobile device management (MDM) and hardening actions (the disabling of unnecessary services, such as securing USB ports in all port systems).
OP-02: Implement device and software whitelists and review the list at least annually or in case of a major system change.	• The organisation manages user privileges by employing whitelisting.	• The organisation has a documented process that provides guidance on software and device whitelisting activities.	• The organisation regularly reviews whitelisting activities and supporting documentation to ensure that appropriate privileges to devices and software applications are valid and accurately maintained.
OP-03: Define a change management process to introduce any new device into the port systems (acceptance tests, validation steps, etc.).	• The organisation evaluates newly procured technologies or equipment before entering them into service. • The organisation employs a change management methodology or process to support modifications to its IT, OT, and information assets.	• Prior to adding, changing, or removing an IT, OT, or communication asset or system critical to the delivery of services, the organisation assesses the asset or system for specific cyber risk impact. • The organisation tests new or modified IT, OT, and communication assets prior to deployment in the organisation's live operating environment.	• The organisation documents all updates and changes to IT, OT, or communication systems following testing and prior to implementation.
OP-04: Ensure all employees and contractors return their end-devices at contract termination and define processes for secure end-devices disposal.	• The organisation's employees return end-devices at service contract termination. • Contractors return end-devices at service contract termination.	• The organisation has a documented process that facilitates end-device return at service life end for all employees. • The organisation has a documented process that facilitates end-device return at service life end for all contractors. • The organisation has a policy that establishes clear end-device disposal protocols.	• The organisation reviews end-device return and disposal activities, processes, and procedures at least annually to ensure effectiveness.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Vulnerabilities management			
OP-05: Define a vulnerability management process to identify asset vulnerabilities, it can be based on automatic and manual tools such as vulnerability scans.	• The organisation identifies vulnerabilities in IT/OT assets.	• The organisation deploys commercially available vulnerability scanning tools to automate the discovery of new and existing threats to its IT/OT networked operating environment.	• The organisation has documented policies, practices, and/or procedures that guide asset vulnerability identification and management activities
OP-06: Define intelligence processes for cybersecurity in order to be aware of newly disclosed vulnerabilities and take quick compensatory actions (network segregation, service disabling, etc.)	• The organisation has one or more business processes, methodologies, and/or mechanisms that facilitate the dissemination of collected cyber risk information to designated stakeholders. • The organisation has established procedures to guide both normal operations and enable rapid incident response actions for administrative and operational environments.	• The organisation has established and documented rules, plans, policies, procedures, and/or written practices that guide all cybersecurity information-sharing activities. • The organisation has established and maintains internal protocols and/or procedures that protect and facilitate the secure sharing of confidential or commercially sensitive information.	• The organisation regularly reviews policies, procedures, and/or directives guiding information sharing activities.
OP-07: Establish tight collaboration of OT and IT departments ensuring that their collaboration with systems business owners, decision-making authorities and other stakeholders is efficient and ensure a homogeneous cybersecurity level for IT and OT.	• OT and IT department personnel collaborate in cybersecurity activities, which also includes proactive communication with data/asset/system owners, decision-making authorities, and other stakeholders.	• The organisation has documented policies and procedures that facilitate regular collaboration between OT and IT departmental personnel in coordinated cybersecurity activities across all operational areas. • OT-IT collaboration procedures define information-sharing protocols for supporting data/asset/system owners, decision-making authorities, and other stakeholders to ensure coordination and consistency of cybersecurity activities across all operational areas.	• To ensure that all OT, IT, data/asset/system owners, decision-making authorities and other stakeholders routinely collaborate, the organisation regularly reviews and revalidates all information sharing policies, alert/exception and escalation procedures, notification protocols, and related communication activities. • The organisation mitigates identified communication gaps among OT and IT department personnel, as well as among all data/asset/system owners, decision making authorities and other key stakeholders, and develops and shares lessons learned about this mitigation.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Human resource security			
OP-08: Ensure professional references and audits of criminal records of key personnel for IT and OT management (system administrators, developers, etc.) and key personnel appointed in security roles such as CISO or DPO.	• The organisation collects and checks professional references of key personnel responsible for the management of IT and OT systems, as well as those in critical security roles, such as the Chief Information Security Officer (CISO) or Data Protection Officer (DPO). • The organisation performs vetting (e.g., drug tests, criminal background checks) of key personnel responsible for the management of IT and OT systems, as well as those in critical security roles, such as the CISO or DPO.	• The organisation performs all vetting activities, including reference checks, drug tests, and criminal background consistent with documented policies.	• The organisation reviews all vetting activities and supporting documentation at least annually to ensure effectiveness and alignment with defined policies and procedures.
OP-09: Develop specific and mandatory cybersecurity training courses for some key population dealing daily with IT and OT (system admins, project managers, developers, security officers, harbor master, etc.).	• The organisation has developed customized cybersecurity training material and courses for key staff areas, including personnel responsible for IT/OT systems. • The organisation's cybersecurity training is mandatory for all employees and occurs at least annually. • The organisation informs visitors, customers, vendors, contractors, and other partners of established cybersecurity policies and/or advisories defining expectations and responsibilities regarding cyber risk concerns and prevention measures prior to their entry to the organisation's facilities. • Cyber risk factors that may impact the organisation's Facility Security or Incident Response and Recovery Plans have been introduced into drills and exercises but not as part of a documented plan.	• The organisation delivers cybersecurity training material and courses for key staff areas, including personnel responsible for IT/OT systems, as part of a documented plan. • The organisation delivers cybersecurity and/or cyber risk awareness training to employees and contractors before granting access to key assets as part of the performance of their assigned responsibilities. • Cybersecurity and/or cyber risk awareness training for administrative personnel is tailored to their job functions and responsibilities. • Cybersecurity and/or cyber risk awareness training for personnel working in a marine facility operating environment with OT assets and systems is tailored to their job functions and responsibilities. • The organisation's cybersecurity and/or cyber risk awareness training program for all staff covers how cyber risks may degrade a port or terminal facility's ability to operate.	• The organisation incorporates cyber risk factors that may impact critical assets or services managed by key suppliers or vendors into drills and exercises designed to test Facility Security and/or Incident Response and Recovery Plans. • The organisation requires contractors to confirm that they have delivered cybersecurity awareness training to personnel prior to their arrival at the organisation's facilities. • The organisation's cybersecurity awareness training content identifies the connection between cyber risk factors and potential impacts to personnel health safety, the environment, and critical system asset security. • The organisation identifies lessons learned during drills and exercises that incorporate potential cyber risk factors when testing security and incident response and recovery plans. • Senior leadership regularly evaluates the performance and effectiveness of the organisation's cyber awareness training program to identify where knowledge gaps may exist and to implement improvements to address those gaps.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
OP-10: Set up a security awareness-raising program to address the whole port ecosystem, focusing first on the main threats (e.g. social engineering).	• All employees (administrative and operations) receive cybersecurity awareness training reflecting both the organisation's operating environment and the broader port ecosystem within which it operates.	• The organisation's cybersecurity and/or cyber risk awareness training program for all employees includes appropriate use of social media and cyber risks related to social media exploitation.	• The organisation manages and monitors cyber risk management activities both internally and across the port ecosystem to identify opportunities for refining training content.
Supply chain management			
OP-11: Strictly control access of third parties to port systems by only granting access on demand, in a specified time window, for a specific purpose, and in a least privileged way	• The organisation restricts third-party access to port systems.	• The organisation manages third-party access to port systems based on documented policies and protocols that define specific time frames, objectives (visit purpose) and strict minimum privilege requirements (least privilege).	• The organisation periodically reviews policies defining third-party access control protocols for accuracy and effectiveness.
OP-12: Clearly define all relevant aspects of the partnership with third parties, including security, within the appropriate agreements and contracts, especially for critical systems provided by third-parties (PCS, CCS, security systems, etc.)	• The organisation maintains agreements and contracts with third parties that include clear descriptions of all goods and/or services procured, relevant terms and service levels, and communication protocols. • Agreements with third parties supporting critical systems (PCS, CCS, security, etc.) include clearly defined security standards and performance requirements.	• The organisation has a documented process that facilitates the annual review of all agreements and contracts with all third parties supporting critical systems (PCS, CCS, security systems, etc.) in order to revalidate the accuracy of all terms and conditions, including security. • All agreements and contracts with third parties supporting critical systems include clearly defined terms and conditions describing breach of security notification procedures.	• Agreements with all third parties supporting critical systems include audit clauses (clauses that allow the organisation to validate that the third-party has implemented cybersecurity best practices consistent with the terms of such agreements).
OP-13: Identify the risks and threats at all levels of the port to define categories of incidents and the potential impacts by using the results of risk analysis, threat intelligence, previous incident history, discussion with other ports, etc.	• The organisation categorizes identified risks and threats to IT/OT systems, as well as to third parties within the port ecosystem. • The organisation evaluates identified risks for impact in all port operational areas.	• The organisation has identified and assigned personnel to collect, prioritize and categorize cybersecurity threat information. • The organisation has a process and/or methodology for analysing and de-conflicting information received from multiple sources.	• The organisation has a documented process and/or mechanism in place (risk registry) to support assigned personnel in interpreting collected cybersecurity vulnerability information for impact to critical IT/OT systems.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
OP-14: Define a policy and procedures for incident detection and reaction including the description of the roles and responsibilities of each stakeholder of the port or state level (if applicable), as well as the coordination method and communicate this to all relevant parties.	• The organisation has identified stakeholder roles and responsibilities for incident detection and response. • The organisation has identified stakeholder roles and responsibilities for incident response communications and coordination.	• The organisation has established documented policies defining stakeholder roles and responsibilities at the port or state level (if applicable) for incident detection, response, communication, and coordination activities. • The organisation has defined and documented procedures for incident detection, response, communication, and coordination activities.	• The organisation reviews documented policies and procedures for incident response, communication, and coordination activities least annually for effectiveness. • The organisation re-validates documented policies defining stakeholder roles and responsibilities at least annually.
OP-15: Improve and keep these (OP-14,15) procedures up-to-date by testing them through training exercise, and identification of new feared events.	• The organisation incorporates cyber incident detection, response, communication, and coordination activities into training exercises.	• The organisation regularly tests documented procedures for incident detection, response, communication, and coordination activities in planned training exercises in order to identify opportunities for improvement. • The organisation tests documented procedures for incident detection, response, communication, and coordination activities in training exercises when new threats are identified in order to identify opportunities for improvement.	• The organisation regularly reviews integrated testing and training activities to identify lessons learned, which it shares among relevant stakeholders.
OP-16: Consider the setup of a Cybersecurity Operations Centre (SOC) including IT and OT environments to support security and cyber incidents. The SOCs of the different stakeholders must collaborate (or can be mutualized) to ensure the detection and reaction of incidents at port level.	• The organisation has a Cybersecurity Operations Centre (SOC) that accommodates IT/OT environments to support security requirements. •	• The organisation has a Cybersecurity Operations Centre (SOC) that supports integrated (cyber-physical) security monitoring for its IT/OT environments. • The organisation has confidential information sharing agreements with port organisations that participate in SOC activities.	• The organisation's Cybersecurity Operations Centre (SOC) relates to similar SOCs to support information sharing and coordinated incident response
OP-17: Define alerting procedures and identify the right contacts for each stakeholder of the port depending on the incident criticality (CISO, port management and board, national authorities, CSIRTs, etc.).	• The organisation has a business process, methodology, tool, or other mechanism(s) that facilitates collection of cyber risk information from selected individuals, port partners, CSIRTs, and/or national authorities. • The organisation has formally identified and designated specific individual(s) who are responsible for coordinating internal information sharing sources and activities.	• The organisation has established agreements with third parties that define information sharing requirements with third parties.	• The organisation has documented information-sharing policies that define performance and (where applicable) compliance oversight requirements.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
OP-18: Implement procedures for incident reporting and continuous improvement	• The organisation performs cyber incident reporting	• The organisation has documented policies and procedures that define cyber incident reporting protocols.	• The organisation regularly reviews incident reporting activities for effectiveness and to identify lessons learned. • The organisation shares lessons learned among stakeholders to support continuous improvement activities.
Control and auditing			
OP-19: Perform regular cybersecurity audits (penetration testing, red team, etc.) to check the application and effectiveness of security measures and assess the level of security of port systems	• The organisation performs penetration tests of its networked operating environment to identify vulnerabilities. • The organisation performs ad hoc reviews of existing security measures for effectiveness.	• The organisation regularly performs penetration tests of networked operating environments in accordance with established security policies and procedures. • The organisation performs Red Team tests against its organisation's IT/OT operating environment to test detection and response capabilities.	• The organisation's senior leadership regularly reviews cyber risk management activities for effectiveness and, when specific gaps and/or vulnerabilities are identified, ensures that the organisation develops, implements, and documents relevant corrective actions. • The organisation performs Red Team assessments that involve integrated cyber-physical attack tactics, techniques and procedures, also referred to as “TTPs”.
OP-20: Perform periodic reviews of network rules, access control privileges and asset configurations.	• Organisational leadership periodically reviews network and networked-asset configurations and access control privileges.	• The organisation has documented policies that facilitate regular reviews of network and networked asset configurations and access control privileges.	• The organisation re-validates requirements for network asset configurations and access controls at least annually.
IT and OT physical protection			
OP-21: Ensure IT and OT systems hosted in the port are protected following established best practices for safety (fire detection, air-conditioning, etc.) and security (access control, CCTV, etc.)	• The organisation has appropriately deployed safety (fire detection) and security (CCTV) systems to adequately protect IT/OT systems.	• The Port Facility Security Plan identifies (or has been updated to identify) safety and security systems that the organisation has deployed to protect IT/OT systems.	• The organisation periodically reviews documentation of IT/OT system maintenance activities to ensure traceability to requirements.
OP-22: Keep traceability of all maintenance operations done on IT and OT physical systems	• The organisation maintains records of all security system maintenance activities, including software and firmware upgrades and patches.	• The organisation maintains maintenance documentation on IT and OT physical systems to ensure traceability of operational requirements, security objectives, and service functionality.	• The organisation periodically reviews documentation of IT/OT system maintenance activities to ensure traceability to requirements.

5.5.3 Technical measures

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Network security			
TP-01: Define network segmentation architecture to limit the propagation of attacks within the port systems and avoid direct access from the Internet to very critical port systems such as VTS/VTMIS and security systems.	• The organisation segments critical port systems (e.g., VTS/VTMIS, security systems) from administrative networks with Internet connectivity.	• The organisation has a documented network architecture that segments critical port systems (e.g., VTS/VTMIS, security systems) from port networks with Internet connectivity.	• The organisation review its network segmentation at least annually (or when a change occurs) to re-validate effectiveness.
TP-02: Perform regular network scans to detect unauthorized and malicious networks (WIFI for example) as well as end-devices acting as bridges between two segregated zones (with interfaces in two network zones for example).	• The organisation performs network scanning to detect unauthorized networks (e.g., Wi-Fi) and devices.	• The organisation has documented policies that provide guidance to stakeholders performing regular network scans.	• The organisation has a documented process facilitating the analysis of log data to support business operations and security activities. • The organisation regularly reviews policies and procedures supporting network scanning activities to ensure effectiveness.
TP-03: Define parametric security, with filtering rules.	• The organisation employs parametric security.	• The organisation defines parametric security with filtering rules.	• The organisation has a documented policy that provides guidance on parametric security definitions and filtering rules applicable to its operating environment.
Access control			
TP-04: Set up centralized tools to manage identities and access rights to the port systems. If different tools are set up, due to diversity of the port stakeholders (Port Authorities, terminal operators, local authorities, third-parties, etc.) and their systems, automatic or manual provisioning can be defined.	• The organisation centrally manages user identities, profiles, and access rights to port systems.	• The organisation has implemented a centralized credentialing system to manage user profiles, identities, and access privileges to port systems. • The organisation centrally manages user identities, irrespective of automatic or manual provisioning capabilities of specific port systems. • The organisation has identified stand-alone tools for specific systems and they inform centralized administration of user credentials.	• The organisation has identity management plans, policies and procedures that define identity management activities. • The organisation has updated its Port Facility Security to include identify management policies and procedures.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-05: Define an Identity & Access Management (IAM) strategy and its associated processes to manage the lifecycle of identities and their access rights (automatic deactivation of accounts, regular review, least privilege principle and segregation of duties, password guidelines, etc.). This strategy must be, as much as possible, built in common with the stakeholders of the port ecosystem.	• The organisation actively manages access rights of port stakeholder identities. • The organisation informs stakeholders of password guidelines. • The organisation issues user credentials based on the principle of least privilege.	• The organisation has a documented identity and access management strategy. • The organisation regularly re-validates user profiles. • The organisation deactivates user credentials upon termination or a change in duties.	• The organisation has documented policies/procedures that facilitate regular re-validation reviews of user identities and access rights to port systems. • The organisation consistently implements identity and access management activities across all areas of the organisation.
TP-06: Forbid as much as possible the use of generic accounts, by enforcing unique and individual accounts in all port systems, especially for sensitive systems (PCS, CCS, TOS, VTS/VTMIS, security systems).	• The organisation employs user accounts that are identity-based, not role-based, for all port systems, especially sensitive systems (PCS, CCS, TOS, VTS/VTMIS, security, etc.).	• The organisation has documented policies that define role-based user accounts as a requirement.	• The organisation regularly reviews and re-validates user accounts for sensitive systems.
TP-07: Enforce, whenever possible, password complexity policies and rules for systems.	• The organisation's passwords force users to apply a minimum number of characters with alpha-numeric complexity.	• The organisation has a documented policy that establishes minimum requirements for password complexity and refresh rules (e.g., every 3 months).	• The organisation reviews its documented password policy and supporting rules at least annually to ensure effectiveness.
TP-08: Implement multi-factor authentication mechanisms for accounts accessing critical applications (especially for PCS, CCS, TOS, VTS/VTMIS) and data (personal data, sensitive operational data such detailed information on vessels, dangerous goods and cargo), and in case of poorly or unprotected environments (external access through Internet for example, third-party access from other corporate networks, etc.).	• The organisation employs multi-factor authentication at least on an ad hoc basis.	• The organisation has implemented multi-factor authentication for all critical applications and systems (i.e. PCS, CCS, TOS, VTS/VTMIS). • The organisation has implemented multi-factor authentication to control access to the organisation's data (e.g., personal data, sensitive operational data regarding vessels, dangerous goods, cargos, financial information, etc.) • The organisation has documented policies and/or procedures that define multi-factor authentication requirements for accessing port systems and networks.	• The organisation regularly reviews documented policies and/or procedures defining multi-factor authentication for effectiveness.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-09: Consider physical access in the access lifecycle (port facilities, port area, buildings, etc.) and define specific measures for remote access.	• The organisation has established physical access security requirements for port/ port facilities, including restricted areas.	• The organisation has documented physical access control requirements within the Port/ Port Facility Security Plan. • The organisation has defined and documented remote access security requirements and protocols for port facilities.	• The organisation periodically re-validates and reviews documentation establishing physical and remote access control requirements for effectiveness.
TP-10: Regularly perform accounts and access right reviews to ensure accesses are still legit, especially for accounts that have access to sensitive data (personal data, sensitive operational data, dangerous goods information, etc.).	• The organisation reviews access rights of stakeholders with access to sensitive data (personal data, sensitive operational data, and dangerous goods).	• The organisation has a documented policy that defines requirements for periodically reviewing access rights of all stakeholders with access to sensitive data. • The organisation has a documented policy that defines access rights to data subject to privacy requirements.	• The organisation evaluates access rights at least annually to ensure effectiveness. • The organisation evaluates access rights reviews at least annually to ensure the effectiveness of privacy controls.
Administration and configuration management			
TP-11: Define installation and configuration policy and rules and establish security baselines to only install needed services and functionalities and authorize essential equipment for the security and the functioning of port systems.	• The organisation employs operational security baselines to protect port systems. • The organisation employs baseline functional configurations for port security equipment and essential systems. • The organisation has established installation configurations of security equipment based on functional requirements.	• The organisation has documented installation and baseline configuration policies for essential security platforms and essential port system equipment.	• The organisation periodically reviews documentation supporting installation and baseline configuration activities to revalidate security platforms and essential port system equipment to ensure ongoing functionality.
TP-12: Set up specific accounts only used by administrators to perform administration operations (installation, configuration, maintenance, supervision, etc.).	• The organisation has dedicated and documented administrator accounts for each system with exclusive privileges for performing administrative operations. • The organisation requires third parties with administrative privileges to comply with its own security policies on managing administrator accounts	• The organisation has defined and documented administrator account lifecycle management processes. • Third party administrator accounts comply with the organisation's account lifecycle management processes and third parties may be asked to provide evidence of compliance.	• The organisation periodically reviews administrator account lifecycle management processes for effectiveness and adherence to plan. • The organisation periodically audits third party administrator accounts for compliance with organisational processes and policies. Administrator account requirements for third parties are integrated in the organisation's procurement processes.
TP-13: Define Privilege Account Management (PAM) process, security requirements on those accounts and rules to manage their lifecycle. Especially enforce this process for third-parties who oversee administration operations.	• The organisation employs Privilege Account Management (PAM) processes to support security requirements • The organisation requires third parties with administrative privileges to follow PAM processes.	• The organisation has defined and documented PAM processes, related security requirements, and lifecycle management rules.	• The organisation periodically reviews documented PAM processes, related security requirements, lifecycle management rules, and supporting procedures for effectiveness and adherence to plan.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-14: Set up, as much as possible, dedicated administration networks to create safe zones, in priority for critical systems (especially for VTS/VTMIS, Radio systems, security systems, etc.).	• The organisation employs additional security policies for accessing critical systems (e.g., VTS/VTMIS, security systems) in networked environments.	• The organisation has established dedicated safe zone(s), separated by a firewall, to support critical systems (e.g., VTS/VTMIS, security systems).	• The organisation has documented policies and procedures that establish dedicated safe zones for critical systems. • The organisation reviews safe zone configurations supporting critical systems for effectiveness at least annually, or whenever a change occurs to the environment.
Threat management			
TP-15: Ensure anti-malware, anti-spam and anti-virus is installed and up to date on all port systems, including desktops and servers.	• The organisation employs and maintains as current anti-malware, anti-spam, and anti-virus on all port systems, including desktops and servers.	• The organisation has a documented policy that defines minimum requirements for anti-malware, anti-spam, and anti-virus implementations on all port systems.	• The organisation periodically reviews anti-malware, anti-spam and anti-virus solutions to ensure they are performing in accordance with requirements.
Cloud security			
TP-16: Define a cloud security assessment method to evaluate the impact and the risks of choosing cloud solutions by considering applicable laws and regulations.	• When considering engaging a cloud solution vendor, the organisation analyses the potential impact and risk to applicable laws and regulations.	• The organisation utilizes a documented security assessment framework to guide stakeholders in evaluating potential cloud solutions for risk and impact related to applicable laws and regulations.	• As part of the security assessment framework the organisation uses in evaluating cloud solution providers, the organisation performs an operational impact analysis to further quantify the potential risks as they relate to applicable laws and regulations.
TP-17: Include, as much as possible, security and availability aspects in agreements with cloud security providers.	• The organisation incorporates language describing minimum-security criteria regarding data access, transmission, storage, and availability terms in all agreements with cloud security vendors.	• The organisation maintains and regularly reviews and updates documented policies defining minimum-security criteria in agreements with cloud security providers.	• The organisation regularly reviews agreements with cloud security providers to ensure that data access, security, transmission, storage, and availability terms are consistent with best practices.
TP-18: Try to include, as much as possible, Cloud solutions in the detection and response mechanisms.	• The organisation applies cloud solutions to support cyber threat detection • The organisation applies cloud solutions to support cyber incident response	• The organisation has incorporated cloud solutions in support of cyber threat detection to its policies and procedures • The organisation has incorporated cloud solutions in its cyber incident response policies and procedures	• The organisation regularly reviews the applicability and performance of applied cloud solutions that support cyber threat detection • The organisation regularly reviews the applicability and performance of applied cloud solutions that support cyber incident response

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
Machine-to-machine security			
TP-19: Implement mechanisms to secure machine-to-machine exchanges (including EDI messages and API mostly used with external stakeholders, such as shipping companies) and provide mutual authentication, integrity and confidentiality with the port systems such as encryption, PKI or digital certificates, integrity checks, digital signature, time stamping, especially when exchanges are done over the Internet.	• The organisation secures machine-to-machine communication exchanges (e.g., EDI messages). • The organisation requires that machine-to-machine communication exchanges via the Internet employ secure authentication protocols, such as encryption, PKI, digital certificates, digital signatures, time stamping, etc.	• The organisation has established documented policies and procedures that define security for all machine-to-machine communications. • The organisation has established documented policies and procedures that define authentication protocols for all Internet-based communications.	• The organisation periodically reviews documented policies and procedures guiding machine-to-machine communications to ensure alignment with the organisation's defined performance requirements.
TP-20: Use communication protocols that include a functionality to detect if all or part of a message is an unauthorized repeat of a previous message	• The organisation's stakeholders employ standardized re-validation procedures to confirm messaging.	• The organisation has clearly established communication re-validation protocols within a documented policy or procedure.	• The communication protocol security process is evaluated periodically to assess effectiveness
Data protection			
TP-21: Implement cryptography procedures and mechanisms to protect confidentiality, authenticity and/or integrity of data in the port systems (at rest, in transit or in use). This measure shall be implemented depending on the data classification done.	• The organisation employs cryptography to protect data confidentiality, authenticity, and/or integrity of port systems.	• The organisation has documented cryptography procedures and mechanisms to protect data confidentiality, authenticity, and/or integrity of port systems (which includes data at rest and in transit).	• The organisation reviews documented cryptography procedures and mechanisms to protect data confidentiality, authenticity and/or integrity of port systems (which includes data at rest and in transit) at least annually for effectiveness.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-22: Anonymize and secure any direct or indirect personal data processed within the company, e.g. through role-based access control and encryption, having considered all relevant legal requirements.	• The organisation anonymizes processed personal data. • The organisation has reviewed all legal requirements regarding data privacy. • The organisation encrypts personal data at rest and in transit.	• The organisation has documented policies and procedures that define security and anonymization requirements for personal data creation, processing, transmission, and storage.	• The organisation regularly reviews all documented policies and procedures managing privacy requirements for personal data for appropriateness and effectiveness.
Update management			
TP-23: Define an update management process to ensure that port IT and OT assets are up-to-date, and, if not possible, apply compensatory measures (network segregation, accounts hardening, etc.), especially for legacy systems (OT systems without any possible update, obsolete but critical applications, etc.).	• The organisation assesses inventoried assets to determine if they are obsolete, and, if so, disables or disconnects them from the network. • The organisation secures obsolete and/or unsupported assets through compensatory security measures (e.g., network segregation).	• The organisation has a documented plan that defines change management policies and configuration management procedures for inventoried assets. • The organisation implements System Development Life Cycle practices to manage assets and systems supporting critical services.	• To ensure adherence to documented performance objectives, the organisation has a process that facilitates the regular monitoring of asset inventorying and change management activities.
TP-24: Verify endpoints' software/firmware authenticity and integrity and ensure tight control over the update.	• The organisation verifies endpoint device software and firmware at deployment and periodically re-validates them thereafter.	• The organisation has documented policies defining endpoint device software and firmware verification and re-validation procedures.	• The organisation periodically reviews documented policies facilitating endpoint device software and firmware verification and re-validation procedures.
TP-25: Verify the source of the update and execute automatic update procedures only if they are based on the risk analysis.	• The organisation verifies software and firmware updates and their sources.	• The organisation evaluates software and firmware updates for cyber risk prior to entering them into service.	• The software and firmware update verification process is reviewed periodically for effectiveness.
Detection and monitoring			
TP-26: Monitor availability of the port systems and devices in real time, where technically feasible, by focusing first on the critical systems and devices such as administration workstations, radio systems and end-devices, VTS/VTMIS, radar systems or security systems and OT end-devices, etc.	• The organisation monitors the availability of critical port systems and devices (e.g., computer workstations, VTS/VTMIS, radar, and security systems)	• The organisation has documented policies and procedures that define technical monitoring requirements for all critical IT/OT systems. • The organisation actively monitors all critical networked IT/OT systems, where feasible.	• The organisation regularly reviews technical monitoring activities for all critical IT/OT systems for effectiveness.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-27: Set up logging system to record events related, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the port systems.	• The organisation performs event logging of access control activities.	• The organisation's event logging of access control activities includes user logon and authentication, access right and security modifications, and asset/device/system access. • The organisation has documented policies and procedures that define event logging and monitoring requirements.	• The organisation regularly reviews event logs. • The organisation regularly reviews documentation governing event logging criteria and monitoring activities to determine effectiveness.
TP-28: Set up log correlating and analysis systems to detect events and contribute to cybersecurity incident detection.	• Organisational stakeholders correlate event logs at least in an ad hoc fashion.	• The organisation has implemented tools (e.g., security information event management) that enable event log correlation and analysis for enhanced cybersecurity detection. • The organisation has identified and assigned individuals to support event correlation activities. • The organisation has documented policies and procedures that define event correlation, analysis, and alerting activities for monitored assets and/or systems.	• The organisation regularly reviews event correlation activities for effectiveness.
Industrial control systems security			
TP-29: Consider OT systems into all the security measures defined in this report to secure as much as possible the industrial control systems and networks. If these cannot be applied, define and implement compensating measures (network segregation, accounts hardening, etc.)	• The organisation segregates all IT and OT networks.	• The organisation has established documented IT/OT network segmentation requirements, including architectures, supporting security measures, policies, controls, and procedures for maintaining organisational configurations.	• The organisation regularly reviews IT/OT network configurations to ensure persistent separation between administrative networks and industrial controls systems and networks supporting operations.
TP-30: Ensure network segmentation between IT and OT systems.	• The organisation segregates all IT and OT networks.	• IT and OT network segregation is not only logical but physical (e.g. separate network devices for IT and OT)	• IT and OT network segregation is tested periodically and evaluated for effectiveness.

Security measure	Examples/evidence for maturity level 1	Examples/evidence for maturity level 2	Examples/evidence for maturity level 3
TP-31: When implementing IoT, consider setting up specific security measures.	• When implementing IoT systems, the organisation secures and centralizes access logs of IoT devices. • When implementing IoT systems, the organisation changes default passwords upon implementation. • When implementing IoT systems, the organisation employs encryption protocols to secure communications. • When implementing IoT systems, the organisation trains staff to recognize security alerts related to IoT endpoints.	• When implementing IoT systems, the organisation has documented secure password policies that provide specific guidance for changing default passwords. • The organisation employs single-sign-on tools to manage access to IoT systems and devices. • When implementing IoT systems, the organisation establishes documented policies defining encrypted protocols for secure communications. • When implementing IoT systems, the organisation implements restrictive network communications policies and sets up virtual LANs.	• When deploying an IoT system, the organisation establishes documented escalation and vulnerability reporting procedures with ongoing vendor support. • When procuring IoT systems, the organisation selects platforms/devices that enable encryption. • When procuring IoT systems, the organisation selects platforms/devices where the vendor has clearly defined secure firmware update policies.
Backup and restore			
TP-32: Set up backups and ensure they are regularly maintained and tested, especially for most central and critical systems, like Active Directory, PCS, CCS, TOS, etc.	• The organisation tests backup systems for critical IT/OT systems.	• The organisation has documented policies and procedures that facilitate maintenance and testing of all backup infrastructure supporting critical IT/OT systems (including Active Directory)	• The organisation regularly reviews backup activities to ensure that they are performed according to relevant plans.

6. SUMMARY

This report offers some practical and actionable good practices to support port operators in conducting effective cyber risk management. Regardless of the framework or methodology used to conduct a cyber risk assessment, port operators are typically confronted by the same challenges related to the complexity of the increasingly integrated IT/OT environment, lack of expertise, security risk management responsibilities split between different operational areas and/or business units, etc. The proposed good practices in this report can be implemented in alignment with any standard risk management methodology, including the framework defined in the ISPS Code, Regulation 725/2004 and Directive 2005/65. Moreover, this report offers practical guidance on how port operators can use the taxonomies introduced in ENISA's 2019 report on Port Cybersecurity to support their cyber risk management activities. Finally, building on the security measures described in the 2019 ENISA report, this document introduces three maturity levels for assessing their organisational cybersecurity capability maturity. Findings derived from these efforts can be used to identify operational vulnerabilities, prioritize security and allocate their cybersecurity resources in a sustainable manner.

People responsible for cyber risk management in port operators can use this document by **tailoring the guidelines, good practices and resources presented for each phase** of the proposed four-phase approach to their own cyber risk management methodologies and operational and organisational context. Moreover, for each phase port operators may consult the relevant list of common challenges to identify those good practices most relevant to their needs. The four phases are:

- Phase 1: Identifying cyber-related assets and services; port operators may use the guidelines, good practices and resources/taxonomies presented here to identify their assets and services that should be addressed in the context of cyber risk management more effectively

- Phase 2: Identifying and evaluating cyber-related risks; port operators may adapt the guidelines, good practices and use the relevant taxonomies in the context of their risk identification and evaluation methodologies.

- Phase 3: Identifying security measures; port operators may use the guidelines, good practices and reference security measures to prioritise those security measures that would be most impactful and practical in the context of their own cyber risk management.

- Phase 4: Assessing cybersecurity maturity; port operators may adapt and employ the proposed model in performing cybersecurity maturity self-assessments for the security measures selected in phase 3, identifying priorities for investing resources for improvement and/or building the programmatic foundations for organisational cybersecurity maturity.

A ANNEX: NATIONAL APPROACHES

In addition to the national transpositions of the EU NIS Directive and of the EU maritime security legislation into their national law, several EU member states have developed and introduced national strategies, guidelines, frameworks or standards that include a cyber risk assessment component, which can be employed by port stakeholders, such as:

- The Baseline Informatiebeveiliging Rijksdienst standard (BIR 2012), in The Netherlands;
- The BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz], Standard -1 Information Security Management Systems (ISMS) and BSI-Standard -2: IT-Grundschutz from the Federal Office for Information Security (BSI) in Germany;
- The Critical Infrastructures Information Protection" (CIIP) Law and the EBIOS Risk Manager Method and related guides[14] from the French Government.
- Controlling the Digital Risk published by ANSSI and AMRAE[15].
- The Danish Cyber and Information Security Strategy[16];
- The Methodology for Information Systems Risk Analysis and Management (MAGERIT)[17] (Spain, Ministry for Public Administrations);
- Guidelines and good practices for cybersecurity risk management in vessels and port facilities (Spain, National Maritime Security Council).

Non-EU countries have also published relevant guidelines, most notably the US Coast Navigation and Vessel Inspection Circular No. 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities[18] and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

[14] See https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf
https://www.ssi.gouv.fr/uploads/2019/04/mapping_the_information_system-anssi-pa-046.pdf
https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf
https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf
https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf
https://www.ssi.gouv.fr/uploads/2014/01/Use_Case_EN.pdf
[15] https://www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/
[16] See https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf
17 See https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html and https://www.pilar-tools.com/doc/magerit/MAGERIT_v_3_%20book_1_method_PDF_NIPO_630-14-162-0.pdf
[18] https://www.federalregister.gov/documents/2020/03/20/2020-05823/navigation-and-vessel-inspection-circular-nvic-01-20-guidelines-for-addressing-cyber-risks-at

B ANNEX: INDUSTRY STANDARDS AND METHODOLOGIES

There are several international or industry standards and risk methodologies that, although not port specific, can be referenced by port stakeholders in their efforts to conduct cyber risk assessments. An indicative list is tabulated in Table 3 below:

Table 3: Standards and methodologies currently used by port stakeholders

Publication	Description
International Organisations	
ISO/IEC 27001:2013	It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.
ISO/IEC 27002:2013	It provides guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).
ISO/IEC 27005:2018	It provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
ISO/IEC 27701:2019	It specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation.
ISO/IEC 28000:2007	It specifies requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management
ISO/IEC 31000 series	The series provide principles, a framework and a process for managing risk. It can be used by any organisation regardless of its size, activity or sector.
ANSI/ISA/IEC 62443 series	The series provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).
ISO 28005-2:2011	The standard contains technical specifications that facilitate efficient exchange of electronic information between ships and shore for coastal transit or port calls. It is intended to cover safety and security information requirements related mainly to the relationships between the ship and the port and coastal state authorities.

HMG IA Standard No 1	Technical Risk Assessment – IA Standard for Risk Managers and IA Practitioners responsible for identifying, assessing and treating the technical risks to ICT systems and services handling HMG information.
Supplier Information Assurance Assessment Framework and Guidance	Guidance on how the Supplier Information Assurance Tool (SIAT) question sets and tool specification can be used by suppliers of key business services to HMG.
Supplier Information Assurance Tool (SIAT) – Summary	A brief summary of the Supplier Information Assurance Tool (SIAT) Community of Interest set up to drive development of a supplier Information Assurance model. ISAB Approved.
Shipping Industry Guidelines	
IMO Guidelines on Maritime Cyber Risk Management	MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. Resolution MSC.428(98)- Maritime Cyber Risk Management in Safety Management Systems encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021
BIMCO Guidelines on Cyber Security Onboard Ships	It is designed to assist shipping companies in formulating their own approaches to cyber risk management on-board ships, providing a risk-based approach to identifying and responding to cyber threats.
DCSA Cybersecurity Implementation Guide	It aims to facilitate vessel readiness for the IMO Resolution MSC.428(98) by providing a task-based approach.
Generic Risk Assessment Methodologies	
CCTA Risk Analysis and Management Method (CRAMM)	It comprises three stages, each supported by objective questionnaires and guidelines. The first two stages identify and analyse the risks to the system. The third stage recommends how these risks should be managed.
Center for Internet Security Risk Assessment Method (CIS RAM)	CIS RAM is an information security risk assessment method that helps organisations implement and assess their security posture against the CIS Controls cybersecurity best practices.
Risk Assessment Matrix (RAM)	It is a project management tool that allows risks to be evaluated in terms of the likelihood or probability of the risk and the severity of the consequences.
Hazard and Operability Study (HAZOP)	It is a structured and systematic examination of a complex planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment
Failure mode and effect analysis (FMEA)	It is an analysis tool used to determine the chance of failure and the ensuing risks in developmental processes of services, products or production methods.
What-if Analysis	It is a tool that runs reverse calculations, sensitivity analysis and scenarios comparison.
Bow-Tie Analysis (BTA)	It is a tool that displays the links between the potential causes, preventative and mitigating controls and consequences of a major incident.
Fault Tree Analysis (FTA)	It is a tool that facilitates the determination of the cause of failure or test the reliability of a system by stepping through a series of events logically.

TP-02-20-790-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-403-9
DOI: 10.2824/671060