Cyber Resilience of Port Infrastructure: An Integrated IMO, ENISA, and IAPH Approach to Critical Asset Protection

H. A. Mooduto[a,*]

[a] *Department of Information Technology, Politeknik Negeri Padang, Kampus Limau Manis, Padang, 25164, Indonesia*
*Corresponding author: *mooduto@pnp.ac.id*

***Abstract*— Seaports have become cyber-physical hubs in which terminal operating systems, port community systems, and operational technology sustain global trade, yet recent incidents such as the 2023 ransomware attack on the Port of Nagoya and the intrusion at DP World Australia show that the loss of a single digital asset can halt national logistics. This study compares and integrates three port cyber guidance instruments: the International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management, the European Union Agency for Cybersecurity (ENISA) port cybersecurity guidelines, and the International Association of Ports and Harbors (IAPH) Cybersecurity Guidelines for Ports and Port Facilities, to derive a coherent model for protecting critical port assets. The materials comprised the official texts of these instruments, the NIST Cybersecurity Framework 2.0, and nine documented port incidents. A directed content analysis was applied using a codebook of 24 control domains grouped under the functions Govern, Identify, Protect, Detect, Respond, and Recover, each scored on a four-level scale. The results show that the instruments are complementary: IMO provides the strongest governance anchor, ENISA the most operational guidance on assets, risks, and technical protection, and IAPH the executive, financial, and continuity perspectives. Integration raises overall coverage from 70.8% to 83.3%, but detection and operational technology recovery remain weak in all instruments. The study proposes an integrated Port Cyber Resilience Framework with a five-level maturity model aligned with Indonesian vital information infrastructure regulation. Further research should validate the framework through port-level maturity assessments and expert panels.**

***Keywords*— Cyber resilience; port infrastructure; critical asset protection; maritime cybersecurity; IMO; ENISA; IAPH.**

I. INTRODUCTION

Seaports are the physical and informational junctions of global trade. Port infrastructures handle more than 80% of the world's cargo by volume [1], and their competitiveness increasingly depends on digital platforms that coordinate vessels, cargo, customs, and hinterland transport. The smart-port paradigm associated with Industry 4.0 has accelerated the deployment of terminal operating systems, port community systems, Internet of Things sensors, automated gates, and remotely operated cranes [2]. These technologies converge information technology (IT) and operational technology (OT) into cyber-physical systems whose compromise can produce safety, environmental, and economic consequences rather than mere data loss [3], [4].

The threat landscape has evolved accordingly. Reviews of maritime cyber incidents show a steady rise in attacks against shipping companies, terminals, and port authorities, with ransomware, network intrusion, and distributed denial-of-service as recurring patterns [5], [6], [1]. Two recent incidents illustrate the systemic stakes. In July 2023, a ransomware attack attributed to LockBit 3.0 disabled the unified terminal system that controls the container terminals of the Port of Nagoya, Japan's busiest port, suspending container handling for about two days [7]. Four months later, an intrusion at DP World Australia forced the operator to disconnect its terminals from the internet; landside freight stopped for three days at terminals handling roughly 40% of the country's container trade, leaving a backlog of some 30,000 containers [8]. In both cases the decisive damage did not arise from the sophistication of the attack but from the absence of resilient operating modes once a central digital asset became unavailable.

Cyber resilience therefore extends beyond preventing attacks to the capacity of a system to prepare for, absorb, recover from, and adapt to adverse cyber events [9]. For ports, this capacity must be built across a heterogeneous ecosystem of public authorities, private terminal operators, shipping lines, logistics providers, and technology vendors, each with different obligations and levels of maturity [10], [11]. Several guidance instruments have emerged to support this effort. The International Maritime Organization (IMO) adopted Resolution MSC.428(98), which required cyber risks to be addressed in safety management systems no later than 1 January 2021 [12], and issued the Guidelines on Maritime Cyber Risk Management, most recently revised as MSC-FAL.1/Circ.3/Rev.3 in April 2025 [13], [14]. The European Union Agency for Cybersecurity (ENISA) published port-specific good practices in 2019 and a four-phase cyber risk management approach for port operators in 2020 [15], [16]. The International Association of Ports and Harbors (IAPH), together with contributors from the World Bank, released its Cybersecurity Guidelines for Ports and Port Facilities in 2021, addressed primarily to senior executives [17].

Although these instruments share the goal of protecting port operations, they originate from different institutional mandates, target different audiences, and adopt different levels of abstraction. Port operators, particularly in developing economies, therefore face a practical question: which elements of each instrument should be adopted, and

how can they be combined without duplication or gaps? Existing scholarship has mapped threats and attack taxonomies [18], [19], [20], [21], proposed model-based risk assessment [22], examined onboard readiness and cyber-physical security assessment of vessels [23], [24], and investigated human factors such as risk perception and the competencies of port facility security officers [25], [26]. Bibliometric reviews confirm that maritime cyber research has grown rapidly but remains fragmented and largely ship-centric, with limited attention to ports as integrated cyber-physical systems and to the governance instruments that regulate them [27], [28], [29]. To the best of the authors' knowledge, no study has systematically crosswalked IMO, ENISA, and IAPH guidance at the level of critical port assets and quantified their complementarity.

The issue is also pressing for Indonesia, an archipelagic state whose economy depends on maritime connectivity. Presidential Regulation No. 82 of 2022 designates transportation as a vital information infrastructure (IIV) sector under the Ministry of Transportation, assigns the National Cyber and Crypto Agency (BSSN) as national coordinator, and requires IIV operators to measure their cybersecurity maturity [30]. BSSN subsequently issued a protection framework for IIV operators [31]. Translating these cross-sector obligations into port-specific practice requires a reference model grounded in international maritime guidance.

This study addresses these gaps with three objectives: (1) to compare the scope and depth of IMO, ENISA, and IAPH guidance using a common functional taxonomy derived from the NIST Cybersecurity Framework (CSF) 2.0 [32]; (2) to quantify the coverage and complementarity of the three instruments and relate the observed gaps to documented port incidents; and (3) to propose an integrated Port Cyber Resilience Framework (PCRF) with a maturity model that can be applied by port operators, including those in Indonesia. Section II describes the materials and method, Section III presents and discusses the results, and Section IV concludes with implications and directions for further research.

II. Materials and Method

A. Research Design

This study adopted a qualitative comparative policy analysis using directed content analysis, an approach suited to examining how normative documents address a predefined set of concepts. A directed approach was chosen because the analytic categories could be derived a priori from an established cybersecurity taxonomy, which ensures comparability across instruments written for different audiences. The research proceeded in six stages, as shown in Fig. 1: corpus selection, codebook development, coding and scoring, incident mapping, synthesis, and framework design.

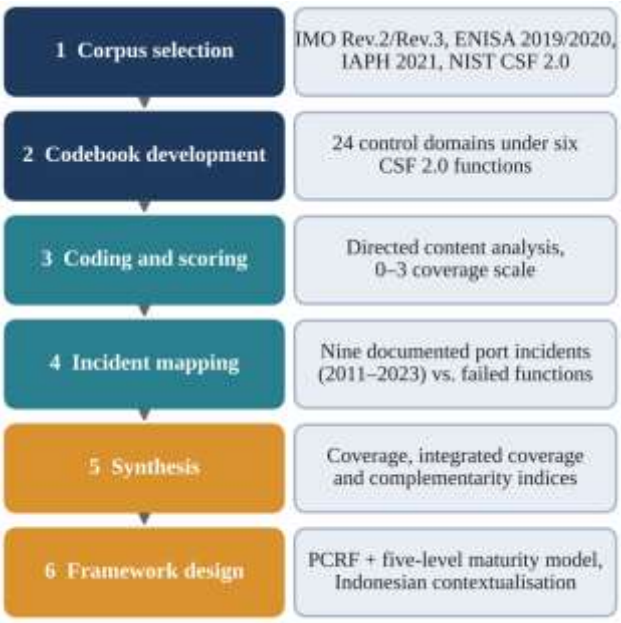


Fig. 1 Research method flow from corpus selection to framework design

B. Materials

The primary corpus consisted of the official, publicly available texts of three instruments. The IMO material comprised Resolution MSC.428(98) and the Guidelines on Maritime Cyber Risk Management in their 2022 (Rev.2) and 2025 (Rev.3) versions [12], [13], [14]. The ENISA material comprised the 2019 report *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector* and the 2020 *Guidelines: Cyber Risk Management for Ports* [15], [16]. The IAPH material comprised Version 1.0 of the *Cybersecurity Guidelines for Ports and Port Facilities*, published on 2 July 2021 [17], complemented by the IAPH guidance on emerging technologies submitted to IMO in 2025 [33]. Inclusion criteria required that a document be issued by an intergovernmental body, a public agency, or a global port industry association; that it address port or port facility cyber risk explicitly or by reference; and that its full text be available in English. Table I summarizes the profile of the three instruments.

TABLE I
PROFILE OF THE ANALYSED INSTRUMENTS

Attribute	IMO	ENISA	IAPH
Issuer	UN specialized agency	EU cybersecurity agency	Global port industry association
Key texts	MSC.428(98); MSC-FAL.1/ Circ.3/Rev.2 and Rev.3	Port Cybersecurity (2019); Cyber Risk Management for Ports (2020)	Cybersecurity Guidelines for Ports and Port Facilities v1.0 (2021)
Audience	Administrations, companies, port facilities	Port authorities, terminal operators, CISOs	Port executives and boards
Status	Non-mandatory; linked to ISM/ISPS	Non-binding; supports NIS/NIS2	Voluntary; referenced in IMO Rev.3
Structure	Functional elements (Govern added in Rev.3)	Four-phase risk approach; good-practice catalogue	Business case, governance, risk, resilience
Level	High-level	Operational	Strategic-managerial

Secondary materials served as reference points. NIST CSF 2.0 provided the neutral analytic taxonomy, because its functions Identify, Protect, Detect, Respond, and Recover are the lineage of the IMO functional elements and because version 2.0 elevated governance to a stand-alone Govern function [32]. Standards for industrial automation and control systems, namely the IEC 62443 series [34], and the EU NIS2 Directive [35] were consulted to interpret technical and regulatory domains. Incident evidence was drawn from peer-reviewed incident reviews [5], [6], [1] and contemporaneous maritime press reports [7], [8].

C. Critical Port Asset Taxonomy

To anchor the analysis on assets rather than on abstract controls, a five-layer taxonomy of critical port assets was constructed from the asset categories in the ENISA guidelines [16], the systems listed in the IMO Guidelines [14], and the port services identified in prior surveys [4], [3]. As illustrated in Fig. 2, the layers progress from enterprise IT (L1), through port community and trade systems (L2) and terminal operations (L3), to operational technology and industrial control systems (L4) and physical security and safety systems (L5). The consequences of compromise shift along this continuum from financial and data loss toward physical damage, safety hazards, and the loss of cargo-handling capacity. Third-party remote access, cloud services, communication links, and people constitute cross-cutting exposures that can propagate an incident across layers.

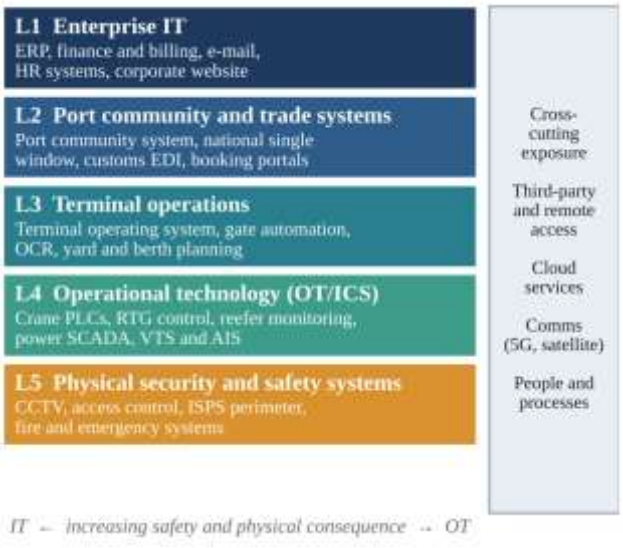


Fig. 2 Five-layer taxonomy of critical port assets with cross-cutting exposure channels

D. Codebook, Coding, and Scoring

The codebook comprised 24 control domains, four under each CSF 2.0 function (Fig. 3 lists all domains). Domains were selected to represent outcomes that are material to port operations, for instance IT/OT segmentation, degraded-mode operation, and coordination across the port community, rather than to replicate every CSF subcategory. For each instrument k and domain i, a coverage score $s_{k,i}$ was assigned on a four-level ordinal scale: 0 (absent), 1 (mentioned without guidance), 2 (guided, i.e., recommended with general direction), and 3 (detailed, i.e., supported by actionable practices, examples, or procedures). Coding was performed on the full texts with an explicit codebook containing decision rules and anchor examples; each score was linked to the supporting section of the source, and ambiguous passages were resolved by consensus among the authors. Where an instrument existed in several versions, the most comprehensive treatment was coded.

The trustworthiness of the qualitative analysis was addressed in three ways. Credibility was supported by linking every score to a traceable passage of the source text, which allows independent verification. Dependability was supported by fixing the codebook, decision rules, and scoring anchors before coding began, so that the same rules were applied to all instruments. Transferability was supported by expressing results in terms of the generic asset layers of Fig. 2 and the functions of CSF 2.0, which are applicable to ports of different sizes and jurisdictions.

Three indices were computed for each function f containing n_f domains (n_f = 4). The coverage index of instrument k measures its relative depth of guidance:

$$CI_{k,f} = \frac{\sum_{i=1}^{n_f} s_{k,i}}{3n_f} \times 100\% \quad (1)$$

The integrated coverage index assumes that a port adopts the strongest guidance available for each domain across the three instruments:

$$IC_f = \frac{\sum_{i=1}^{n_f} max_k\, s_{k,i}}{3n_f} \times 100\% \quad (2)$$

The complementarity gain quantifies how much integration improves on the best single instrument:

$$G_f = IC_f - max_k\, CI_{k,f} \quad (3)$$

A gain of zero indicates that one instrument already provides the best available guidance for every domain of the function, whereas a low integrated index reveals a gap that cannot be closed by combining the three instruments and therefore requires external standards.

E. Incident Mapping

Nine publicly documented incidents affecting ports or terminal operators between 2011 and 2023 were selected from incident reviews and press reports [5], [6], [1], [7], [8]. Selection favoured incidents with sufficient public detail on attack vector, operational impact, and recovery. For each incident, the CSF function whose weakness most visibly determined the magnitude of disruption was identified, providing an empirical lens through which to interpret the coverage gaps.

III. Results and Discussion

A. Orientation of the Three Instruments

The three instruments differ markedly in orientation. The IMO Guidelines provide high-level recommendations and functional elements intended to be embedded in existing risk management processes, including the safety management systems required by the ISM Code and the security plans required under the ISPS Code [13]. The 2025 revision introduced a Govern function and refined definitions such as computer-based systems, aligning the IMO approach with CSF 2.0 and widening attention to the maritime digital ecosystem, including port facilities [14]. Its strength lies in normative legitimacy: as an IMO circular, it is recognized by maritime administrations worldwide and serves as the reference point for national regulators and industry guidance.

ENISA adopts an operational perspective. Its 2019 report catalogues port-specific threats and good practices, emphasizing governance that involves all port stakeholders, enforcement of technical basics such as network segregation, update management, and segregation of rights, security by design, and detection and response capabilities at port level [15]. The 2020 guidelines add a four-phase approach in which operators identify assets and services, identify and evaluate cyber risks, identify security measures, and assess cybersecurity maturity, and the approach is designed to be adapted to whatever risk methodology an operator already follows [16]. ENISA is consequently the most prescriptive of the three on technical controls.

IAPH, by contrast, addresses the executive layer. Developed by 22 experts from member ports together with World Bank contributors, the guidelines help port organizations establish the financial, commercial, and operational impact of a cyber-attack, assess their readiness to prevent, stop, and recover from attacks, and determine the resources required for effective cyber risk management [17]. They frame cybersecurity as a leadership and business continuity challenge, emphasizing board responsibilities, a cybersecurity steering committee, and the management of the human element, which the guidelines regard as a universal challenge regardless of a port's level of digitalization. IAPH has since extended this work to emerging technologies such as quantum computing and green energy systems [33].

B. Coverage and Complementarity

Fig. 3 presents the coverage scores of the 24 domains, and Table II summarizes the indices per function. Overall, ENISA attained the highest coverage (CI = 70.8%), followed by IAPH (65.3%) and IMO (55.6%). When the strongest guidance for each domain was combined, integrated coverage reached 83.3%, a gain of 12.5 percentage points over the best single instrument. These aggregate figures, however, conceal distinct functional profiles.

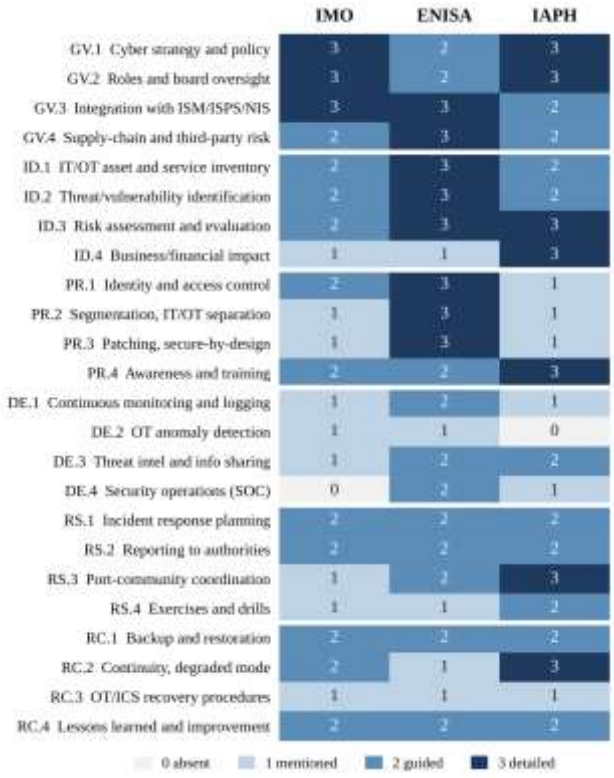


Fig. 3 Coverage scores of the 24 control domains in the IMO, ENISA, and IAPH instruments (0 = absent, 3 = detailed)

TABLE II
Coverage Indices per Function (%)

Function	IMO	ENISA	IAPH	IC	G
Govern	91.7	83.3	83.3	100.0	8.3
Identify	58.3	83.3	83.3	100.0	16.7
Protect	50.0	91.7	50.0	100.0	8.3
Detect	25.0	58.3	33.3	58.3	0.0
Respond	50.0	58.3	75.0	75.0	0.0
Recover	58.3	50.0	66.7	66.7	0.0
Overall	**55.6**	**70.8**	**65.3**	**83.3**	**12.5**

In Govern, all three instruments scored highly, with IMO strongest (91.7%), reflecting the explicit treatment of governance in Rev.3 and its anchoring in ISM and ISPS obligations. IAPH complemented IMO on board oversight and strategy, whereas ENISA contributed the most detailed guidance on supply-chain risk, including supplier remote access and the lack of security certification for port products.

In Identify and Protect, ENISA dominated with 83.3% and 91.7%, respectively, offering detailed practices on asset inventories, threat scenarios, network segmentation, and patch management. IAPH filled one important gap: it was the only instrument to treat business and financial impact quantification in depth (ID.4), which is essential for justifying security investment to executives. Integration therefore raised Identify and Protect to full coverage and produced the largest complementarity gain in Identify (16.7 points).

The pattern reverses in Respond and Recover, where IAPH led with 75.0% and 66.7%. Its emphasis on coordination across the port community, exercises, and business continuity, including the ability to continue operating in a degraded mode, addresses precisely the capabilities whose absence prolonged the Nagoya and DP World disruptions. Nevertheless, the complementarity gain in these functions was zero, meaning that IAPH alone already provides the best available guidance and that the remaining shortfall is shared by all three instruments.

Detect emerged as the weakest function. The best single instrument, ENISA, reached only 58.3%, IMO reached 25.0%, and integration produced no gain. OT anomaly detection (DE.2) was at best mentioned, and a dedicated security operations capability (DE.4) was absent from IMO. Recovery of OT and industrial control systems (RC.3) was likewise only mentioned by all three. These findings reveal a structural blind spot: guidance designed for policy makers and executives naturally addresses governance and continuity, but the engineering-level capabilities needed to observe and restore crane controllers, terminal automation, and power systems lie outside its scope. The gap mirrors the research literature, in which maritime security monitoring is still described as an understudied field with limited datasets and evaluation practice [29], and it explains why ports must turn to industrial control system standards such as IEC 62443 [34] to complete their programmes.

C. Coverage Across Asset Layers

Reading the coverage results against the asset taxonomy of Fig. 2 clarifies where each instrument offers the most value. The IMO Guidelines enumerate vulnerable systems mainly from a ship perspective and reach port facilities through the ISPS Code, so their guidance is most directly applicable to enterprise IT (L1) and to the access control and surveillance systems of the security layer (L5). ENISA explicitly addresses the systems that characterize a port, including terminal operating systems, port community systems, and industrial equipment, and therefore provides the richest guidance for layers L2 to L4. IAPH treats assets primarily through their business value and their role in the port community, which makes it most useful for prioritizing L1 and L2 and for coordinating stakeholders who share these systems.

The layer perspective also explains why recent incidents were so disruptive. The system compromised at Nagoya was a terminal operations platform (L3) that controlled all container terminals of the port [7], while the DP World Australia response required the operator to sever the internet connectivity on which its gate and landside operations depended [8]. Both events struck the L2 and L3 layers that convert digital transactions into physical cargo flows, precisely where guidance on detection and degraded-mode operation is weakest. Ports should therefore prioritize L3 and L4 assets when allocating monitoring and recovery resources, even though enterprise IT usually attracts the largest share of cybersecurity budgets.

These findings are consistent with, and extend, prior research. Earlier reviews described the maritime threat landscape and attack taxonomies qualitatively [18], [4], [20], and studies of the European port sector attributed vulnerability largely to a lack of cybersecurity awareness [10]. The present analysis complements these threat-oriented studies by examining the guidance side, showing that the weaknesses observed in practice correspond to gaps in the instruments themselves. It also confirms, from a policy perspective, the call by Afenyo and Caesar for stronger education and training [21], and it shows that asset-based risk modelling, as proposed in the MaCRA framework [22], needs to be paired with explicit detection and recovery capabilities at the OT layer.

D. Lessons from Port Incidents

Table III maps the nine incidents to the function whose weakness most visibly shaped the outcome. Two observations stand out. First, the dominant failure mode shifted over time from integrity breaches exploited for smuggling, as in the Antwerp case, to availability attacks against central operating platforms, which is consistent with the predominance of ransomware reported in port incident reviews [6], [1]. Second, in most disruptive cases the critical weakness lay not only in Protect but in Respond and Recover: once a central platform such as a terminal operating system was compromised, operators lacked tested manual or degraded procedures, restoration took days, and economic losses propagated to shippers and hinterland logistics [7], [8]. Conversely, the 2021 attempted intrusion at the Port of Houston, which was detected and contained before operational impact [6], demonstrates the value of early detection, the very function that the guidance instruments cover least.

TABLE III
SELECTED PORT CYBER INCIDENTS AND THE WEAKEST RESILIENCE FUNCTION

Incident (year)	Vector	Operational impact	Weakest function
Port of Antwerp (2011–13)	Intrusion by smugglers into container systems	Manipulated container data used for drug trafficking	Protect, Detect
Maersk / APM Terminals (2017)	NotPetya wiper via compromised software update	Global terminal disruption; manual operations	Protect, Recover
Port of San Diego (2018)	Ransomware on IT systems	Administrative services disrupted	Recover
Shahid Rajaee, Iran (2020)	State-linked attack on port computers	Vessel and truck congestion	Detect, Respond
Transnet, South Africa (2021)	Cyber-attack on IT systems	Force majeure at container terminals	Respond, Recover
Port of Houston (2021)	Zero-day in a password management tool	Contained; no operational impact	Detect (effective)
Port of Lisbon (2022)	LockBit ransomware	Website and data affected	Protect
Port of Nagoya (2023)	LockBit 3.0 ransomware on terminal system	Container handling halted about two days	Recover
DP World Australia (2023)	Unauthorized network access	Three-day stop; ~30,000 containers delayed	Respond, Recover

Sources: [5], [6], [1], [7], [8].

E. Integrated Port Cyber Resilience Framework

Building on the coverage analysis, the PCRF assigns each function to the instrument that provides the strongest guidance and supplements the functions in which integration leaves gaps (Fig. 4). The framework is organized in four tiers. The top tier comprises the normative anchors that legitimize a port cyber programme: the IMO Guidelines, the ISPS Code through the port facility security assessment (PFSA) and plan (PFSP), the NIS2 Directive for European ports [35], and, for Indonesian ports, Presidential Regulation 82/2022 and BSSN Regulation 8/2023 [30], [31]. The second tier is Govern, anchored on IMO Rev.3 and enriched by the board-level practices of IAPH. A distinctive element is the integration of the chief information security officer role with that of the port facility security officer, responding to evidence that port facility security officers often lack cyber competencies while IT staff lack an understanding of port security regimes [26], [36].

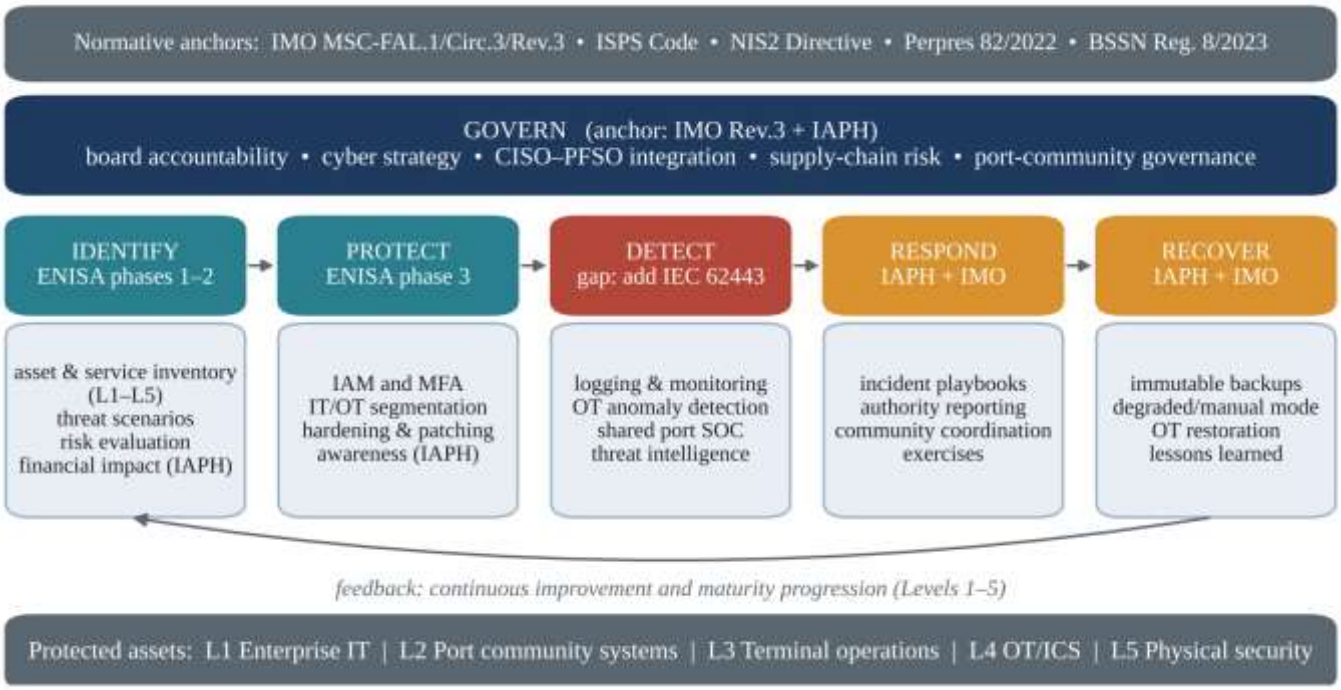


Fig. 4 Integrated Port Cyber Resilience Framework (PCRF) synthesizing IMO, ENISA, and IAPH guidance, with IEC 62443 closing the detection gap

The third tier operationalizes the five remaining functions. Identify and Protect adopt the four-phase approach and technical good practices of ENISA, extended with the financial impact assessment of IAPH so that risk results can be expressed in terms on which executives and boards act. Detect, the gap identified in Section III-B, is completed with the zone-and-conduit segmentation and monitoring requirements of IEC 62443 and with a shared security operations capability for the port community, an arrangement that can make continuous monitoring affordable for smaller terminal operators. Respond and Recover follow IAPH and IMO, emphasizing incident playbooks, timely reporting to authorities, joint exercises with the port community, immutable backups, and pre-tested degraded or manual modes for terminal and gate operations. The bottom tier ties all practices to the five asset layers of Fig. 2, so that controls are prioritized according to operational consequence, while a feedback loop links lessons learned to maturity progression.

Human factors cut across all tiers. Phishing and other social engineering techniques are repeatedly reported as initial access vectors in maritime incidents, and the way personnel perceive cyber risk shapes their behaviour [18], [20], [25]. The PCRF therefore treats awareness and role-

specific training both as a Protect domain and as a governance responsibility, in line with the emphasis of IAPH on managing the human element.

F. Maturity Model

To make the PCRF actionable, a five-level maturity model was defined (Fig. 5 and Table IV). Level 1 (Initial) describes ports in which cybersecurity is ad hoc, reactive, and limited to enterprise IT. Level 2 (Developing) introduces a formal policy, an asset inventory spanning the five layers, and basic cyber hygiene. Level 3 (Defined) integrates cyber risk into the PFSA, separates IT from OT networks, and establishes a documented incident response plan. Level 4 (Managed) adds continuous monitoring of OT networks, a security operations capability, and regular port-community exercises measured by performance indicators. Level 5 (Resilient) represents threat-informed operations in which degraded-mode procedures have been proven in exercises and threat intelligence is routinely shared with sector peers. The levels are cumulative, and the maturity assessment phase of ENISA [16] can serve as the evaluation procedure. In Indonesia, the model can be aligned with the cybersecurity maturity measurement that Presidential Regulation 82/2022 requires of IIV operators [30].

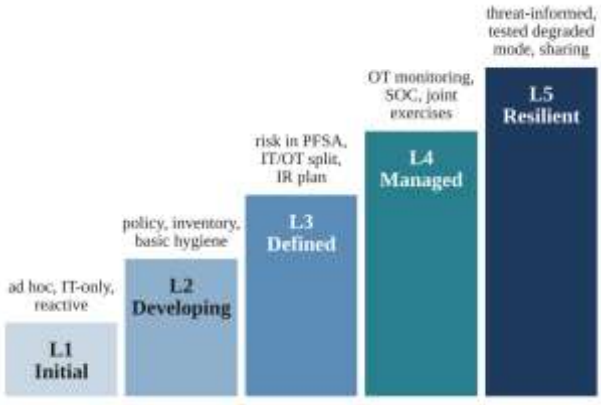


Fig. 5 Five-level port cyber resilience maturity model

TABLE IV
MATURITY LEVELS AND INDICATIVE VERIFICATION EVIDENCE

Level	Indicative evidence
L1 Initial	No approved cyber policy; incidents handled ad hoc by IT staff
L2 Developing	Approved policy; L1–L5 asset register; MFA for remote access; awareness programme
L3 Defined	Cyber risk in PFSA/PFSP; IT/OT zones and conduits; tested backups; incident response plan
L4 Managed	OT network monitoring; dedicated or shared SOC; annual port-community exercise; indicators reported to the board
L5 Resilient	Proven degraded-mode drills; threat-intelligence sharing via CSIRT/ISAC; continuous improvement cycle

G. Implications for Indonesian Ports

Three implications follow for Indonesia. First, the consolidation of the state-owned port operators into a single integrated operator in 2021 improved operational efficiency but also concentrated digital dependencies. As the DP World Australia case shows, a single intrusion into a national-scale operator can paralyse a large share of a country's container trade [8]; shared platforms should therefore be designed with segmentation between regional terminals and with regional fallback capabilities. Second, the IIV regime provides the legal basis for adoption. The Ministry of Transportation, as sector authority, and BSSN, as coordinator, could adopt the PCRF domains as a port-specific profile of the national protection framework [30], [31], and port facility security assessments under the ISPS Code could incorporate the asset layers of Fig. 2. Third, the skills gap is a binding constraint. Studies show that port facility security officers and maritime graduates receive insufficient cyber training [26], [21]. Vocational institutions in port regions, such as the polytechnics of West Sumatra, which hosts the Port of Teluk Bayur, are well placed to deliver applied curricula on OT security, incident response, and port-community exercises in partnership with port operators and BSSN.

H. Limitations

This study has limitations. The coverage scores reflect expert interpretation of policy texts and, although a structured codebook was used, remain ordinal judgments; future replications should report inter-rater reliability statistics. The instruments are living documents: IMO is discussing further steps to strengthen cybersecurity measures for ships and port facilities, and IAPH continues to extend its guidelines, so coverage will change over time. Finally, the PCRF and its maturity model have not yet been validated empirically within port organizations.

IV. CONCLUSION

This study compared the IMO, ENISA, and IAPH approaches to port cybersecurity through a common CSF 2.0 taxonomy and a five-layer critical asset model. The results show that the instruments are complementary rather than redundant. IMO provides the normative anchor and the strongest governance guidance, ENISA offers the most operational guidance for identifying assets and risks and for protecting systems, and IAPH contributes the executive, financial, and continuity perspectives that dominate response and recovery. Combining the strongest guidance from each instrument raises overall coverage from 70.8% for the best single instrument to 83.3%. However, detection and the recovery of operational technology remain weak across all three instruments and cannot be closed by integration alone, a gap that the incidents at Nagoya and DP World Australia have shown to be decisive.

The proposed Port Cyber Resilience Framework and its five-level maturity model translate these findings into an actionable reference that can be aligned with national regimes, including Indonesia's vital information infrastructure regulation. For further research, the framework should be validated through maturity assessments in operating ports, expert panels using Delphi or analytic hierarchy methods to weight the domains, and quantitative modelling of the economic benefit of degraded-mode capabilities. Extending the analysis to emerging technologies such as autonomous handling equipment, private 5G networks, and artificial intelligence in terminal operations would also be valuable.

ACKNOWLEDGMENT

The authors thank the Center for Research and Community Service (P3M) of Politeknik Negeri Padang for supporting this research.

REFERENCES

[1] M. Badea, O. Bucovețchi, A. V. Gheorghe, and G. Raicu, "Cyberattacks on port infrastructures: A decade of trends, incidents, and mitigation strategies (2011–2024)," *Land Forces Acad. Rev.*, vol. 30, no. 2, pp. 175–189, 2025, doi: 10.2478/raft-2025-0017.

[2] A. Paraskevas, M. Madas, V. Zeimpekis, and K. Fouskas, "Smart ports in Industry 4.0: A systematic literature review," *Logistics*, vol. 8, no. 1, 2024, Art. no. 28, doi: 10.3390/logistics8010028.

[3] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber physical systems security for maritime assets," *J. Mar. Sci. Eng.*, vol. 9, no. 12, 2021, Art. no. 1384, doi: 10.3390/jmse9121384.

[4] M. A. Ben Farah *et al.*, "Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022, Art. no. 22, doi: 10.3390/info13010022.

[5] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav, Int. J. Mar. Navig. Saf. Sea Transp.*, vol. 15, no. 3, pp. 519–530, 2021, doi: 10.12716/1001.15.03.04.

[6] C. Senarak, "Port cyberattacks from 2011 to 2023: A literature review and discussion of selected cases," *Marit. Econ. Logist.*, vol. 26, pp. 105–130, 2024, doi: 10.1057/s41278-023-00276-8.

[7] The Maritime Executive. (2023, Jul. 5). *Ransomware attack stops container operations at Japan's Nagoya port*. [Online]. Available: https://maritime-executive.com/article/ransomware-attack-stops-container-operations-japan-s-nagoya-port

[8] The Maritime Executive. (2023, Nov. 13). *DP World Australia resumes terminal ops after "serious" cyber incident*. [Online]. Available: https://maritime-executive.com/article/dp-world-australia-resumes-terminal-ops-after-serious-cyber-incident

[9] I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," in *Cyber Resilience of Systems and Networks*, A. Kott and I. Linkov, Eds. Cham, Switzerland: Springer, 2019, pp. 1–25, doi: 10.1007/978-3-319-77492-3_1.

[10] M. Bocayuva, "Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic," *WMU J. Marit. Affairs*, vol. 20, 2021, doi: 10.1007/s13437-021-00240-4.

[11] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," *Transp. Res. Procedia*, vol. 45, pp. 547–554, 2020, doi: 10.1016/j.trpro.2020.03.058.

[12] International Maritime Organization, "Maritime cyber risk management in safety management systems," Resolution MSC.428(98), London, U.K., Jun. 16, 2017.

[13] International Maritime Organization, "Guidelines on maritime cyber risk management," MSC-FAL.1/Circ.3/Rev.2, London, U.K., Jun. 7, 2022.

[14] International Maritime Organization, "Guidelines on maritime cyber risk management," MSC-FAL.1/Circ.3/Rev.3, London, U.K., Apr. 4, 2025.

[15] European Union Agency for Cybersecurity (ENISA), "Port cybersecurity: Good practices for cybersecurity in the maritime sector," ENISA, Heraklion, Greece, Nov. 2019.

[16] European Union Agency for Cybersecurity (ENISA), "Guidelines: Cyber risk management for ports," ENISA, Athens, Greece, Dec. 2020, doi: 10.2824/671060.

[17] International Association of Ports and Harbors (IAPH), "Cybersecurity guidelines for ports and port facilities," Version 1.0, IAPH, Tokyo, Japan, Jul. 2, 2021.

[18] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity challenges in the maritime sector," *Network*, vol. 2, no. 1, pp. 123–138, 2022, doi: 10.3390/network2010009.

[19] B. Mednikarov, Y. Tsonev, and A. Lazarov, "Analysis of cybersecurity issues in the maritime industry," *Inf. Secur. Int. J.*, vol. 47, no. 1, pp. 27–43, 2020, doi: 10.11610/isij.4702.

[20] M. V. Clavijo Mesa, C. E. Patino-Rodriguez, and F. J. Guevara Carazas, "Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains," *Information*, vol. 15, no. 11, 2024, Art. no. 710, doi: 10.3390/info15110710.

[21] M. Afenyo and L. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean Coast. Manag.*, vol. 236, 2023, Art. no. 106493, doi: 10.1016/j.ocecoaman.2023.106493.

[22] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU J. Marit. Affairs*, vol. 18, no. 1, pp. 129–163, 2019, doi: 10.1007/s13437-019-00162-2.

[23] K. Kanwal *et al.*, "Maritime cybersecurity: Are onboard systems ready?," *Marit. Policy Manag.*, vol. 51, no. 3, pp. 484–502, 2024, doi: 10.1080/03088839.2022.2124464.

[24] I. Progoulakis *et al.*, "Cyber–physical security assessment for maritime vessels: Study on drillship DP system using American Petroleum Institute security risk analysis and bow-tie analysis," *J. Mar. Sci. Eng.*, vol. 12, no. 10, 2024, Art. no. 1757, doi: 10.3390/jmse12101757.

[25] M. H. Larsen, M. S. Lund, and F. B. Bjørneseth, "A model of factors influencing deck officers' cyber risk perception in offshore operations," *Marit. Transp. Res.*, vol. 3, 2022, Art. no. 100065, doi: 10.1016/j.martra.2022.100065.

[26] C. Senarak, "Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and port security professionals," *Asian J. Shipp. Logist.*, vol. 37, no. 4, 2021, doi: 10.1016/j.ajsl.2021.10.002.

[27] T. Mawer, S. von Solms, and J. Meyer, "Identifying the scope of cybersecurity research conducted in the maritime industry: 2003–2023," in *Proc. 19th Int. Conf. Cyber Warfare Secur. (ICCWS)*, vol. 19, no. 1, 2024, doi: 10.34190/iccws.19.1.2037.

[28] A. V. Harish *et al.*, "Literature review of maritime cyber security: The first decade," *Marit. Technol. Res.*, vol. 7, no. 2, 2025, Art. no. 273805.

[29] R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi, "A systematic literature review of cyber security monitoring in maritime," *IEEE Access*, vol. 13, pp. 85307–85329, 2025, doi: 10.1109/ACCESS.2025.3567385.

[30] Republic of Indonesia, "Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure," State Gazette of the Republic of Indonesia 2022 No. 129, Jakarta, Indonesia, May 24, 2022.

[31] National Cyber and Crypto Agency (BSSN), "BSSN Regulation No. 8 of 2023 on the Vital Information Infrastructure Protection Framework," BSSN, Jakarta, Indonesia, 2023.

[32] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Gaithersburg, MD, USA, Feb. 26, 2024, doi: 10.6028/NIST.CSWP.29.

[33] International Association of Ports and Harbors (IAPH), "IAPH cyber resilience guidelines for emerging technologies," submitted to the IMO Maritime Safety Committee, document MSC 110/7/1, London, U.K., 2025.

[34] *Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels*, IEC 62443-3-3, International Electrotechnical Commission, Geneva, Switzerland, 2013.

[35] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," *Off. J. Eur. Union*, vol. L 333, pp. 80–152, Dec. 27, 2022.

[36] C. Senarak, "Port cybersecurity and threat: A structural model for prevention and policy development," *Asian J. Shipp. Logist.*, vol. 37, no. 1, 2021, doi: 10.1016/j.ajsl.2020.05.001.