Regulatory Challenges in Maritime Cybersecurity: Evidence from Expert Workshops

Bilge Karabacak, Kasey Miller, Ulku Clark, Jeff Cummings, Edwin Garces and Geoff Stoker
Congdon School of Supply Chain, Business Analytics, & Information Systems, Cameron School of Business, Wilmington, NC, USA

karabacakb@uncw.edu
millerkc@uncw.edu
clarku@uncw.edu
cummingsj@uncw.edu
garcese@uncw.edu
stokerg@uncw.edu

Abstract: The maritime transportation sector is crucial for nations worldwide, as the Maritime Transportation System (MTS) facilitates over 90% of international trade through an extensive network of ships and ports. As digitized maritime operations become increasingly prevalent, advanced technologies are being integrated into these systems. MTS's critical importance, along with its dependence on interconnected systems and new digital technologies, renders it vulnerable to cyberattacks at ports and other key points. Consequently, implementing cybersecurity regulations in the maritime sector is essential to ensure operational safety and security. However, organizations within this sector encounter significant challenges in adopting and adapting to these regulations, highlighting the need for robust, clear, and enforceable standards. Previous studies have identified various gaps and challenges in maritime cybersecurity regulations, including fragmented, outdated, and inconsistent enforcement. To address these issues, this paper employs a qualitative analysis through expert workshops to evaluate whether the findings effectively reflect real-world experiences with operational and regulatory applications. The study aims to identify and analyze gaps and challenges in existing regulations, policy standards, and frameworks for maritime cybersecurity.

Keywords: Maritime cybersecurity, Regulations, Standards, Frameworks, Qualitative data analysis, Expert elicitation, Cyber resilience

1. Introduction

Maritime logistics is a crucial component of global business and freight, encompassing over 90% of world trade and more than 50,000 ships (Drummond and Machado, 2021). Consequently, the integration of emerging maritime technologies has led to a surge in novel cybersecurity threats. The accelerated digitalization of systems has not been met with proper and prompt debugging, release, and regulation (Hopcraft and Martin, 2018; Karim, 2022; Dimakopoulou and Rantos, 2024). Regulations, standards, and frameworks do not always align with real-world practice, causing contradictory diagrams, procedures, and limited integration among voluntary frameworks.

However, regulations, standards, and frameworks are crucial for preventing cybersecurity attacks. They serve as primary sources for security requirements and controls, helping organizations establish robust defenses, protect data, and mitigate risks. Adherence to these requirements supports consistent security practices and builds trust among partners, customers, and stakeholders (Taherdoost, 2022). Furthermore, mandatory and optional frameworks provide essential guidance to support national security and raise awareness of cybersecurity risks (Djebbar and Nordstrom, 2023; Amin, 2024; Folorunso, Mohammed, et al., 2024; Folorunso, Wada, et al., 2024).

One challenge in maritime cybersecurity is the lack of regulatory specificity for particular fields or sectors. Non-tailored regulations can lead to inefficient operations, non-compliance, reduced control, and increased vulnerability, resulting in data breaches, financial losses, and reputational damage (Olney, 2023; Anchore, 2025).

Each sector operates differently and has unique vulnerabilities; consequently, cybersecurity requirements also differ (Miller, 2024). Regulations therefore need to be tailored to specific domains, particularly as automation and new technologies increase system complexity (Heckman et al., 2017; Dimakopoulou and Rantos, 2024). While compliance with standards remains essential, the development and adaptation of effective standards remain unresolved challenges.

Several authors note that experts face difficulties interpreting fragmented and unevenly applied rules, especially when multiple frameworks coexist across national and international contexts (Hopcraft and Martin, 2018; Drazovich, Brew, and Wetzel, 2021; Melnyk, Drozdov, and Kuznichenko, 2025). This underscores the need for

studies identifying gaps and challenges to support harmonized and well-structured regulatory systems (Hopcraft and Martin, 2018; Karim, 2022).

Collecting input from maritime cybersecurity professionals is critical because it provides practical insights that theory or policy alone cannot capture. These insights highlight problems, gaps, and unmet requirements in maritime transportation system regulations (Park et al., 2023). Accordingly, we organized two Maritime Technology Road Mapping (TRM) workshops in January and March 2025 (Clark et al., 2025), interviewing 38 experts from government, NGOs, and the private sector. This study analyzes regulatory challenges identified in these workshops and categorizes regulatory gaps to inform the development of more robust and standardized frameworks.

2. Literature Review

The literature review is organized into two subsections. In the first subsection, we provide an overview of the current cybersecurity regulations, standards, and frameworks in the maritime sector. In the second subsection, we present experts' perspectives on the need for regulatory improvements.

2.1 Regulations, Standards, and Frameworks in Maritime Cybersecurity

The documentation on maritime cybersecurity can be categorized into international instruments, national and international standards, and specialized assessment frameworks.

For international instruments, the International Maritime Organization (IMO) plays a central role. IMO established Resolution MSC.428(98), mandating the inclusion of cyber risk management in Safety Management Systems (SMS), and issued non-mandatory high-level guidelines (Cyber Risk Management – MSC-FAL.1/Circ. 3). Existing codes include the International Ship and Port Facility Security (ISPS) Code and the ISM Code for safety management (Hopcraft and Martin, 2018; Svilicic et al., 2019; Chupkemi and Mersinas, 2024).

National and international standards include the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 2.0, a widely recognized resource for cybersecurity management. NIST CSF 2.0 consists of six functions: Govern, Identify, Protect, Detect, Respond, and Recover. Another key source of guidance comes from classification societies and industry organizations such as BIMCO, DNV-GL, the International Association of Classification Societies (IACS), and the American Bureau of Shipping (ABS). IACS provides specific cyber-related requirements through UR E26 (Cyber Resilience of Ships) and UR E27 (Cyber Resilience of Onboard Systems and Equipment). UR E26, adopted in 2022, establishes minimum cyber-resilience requirements at the ship level, while UR E27 defines cybersecurity requirements for onboard systems, including secure development and vendor obligations. Both requirements are enforced for newbuild ships from July 1, 2024 (IACS, 2022b, 2022a).

Specialized assessment frameworks have been evaluated in studies proposing targeted approaches for maritime cybersecurity. For ships, the Maritime Cyber Risk Assessment (MaCRA) model quantifies cyber risks based on system vulnerabilities, ease of exploitation, and attacker rewards (Tam and Jones, 2019). Other proposed frameworks include Cyber Resilience Evaluation models aligned with UR E26, the NIST CSF, the MITRE Cyber Resiliency Engineering Framework, and the Ship Cyber Risk Assessment Framework (Ko, Lee, and Seo, 2025). The Threat-Informed Defense-in-Depth approach combines threat-informed defense and layered security strategies, particularly for autonomous passenger ships (Amro and Gkioulos, 2023; Wu et al., 2023; Dimakopoulou and Rantos, 2024).

While these frameworks focus on vessels, other models address ports and critical infrastructure. These include the Integrated Cyber Risk Assessment (ICSRA), which applies ISO 31000, NIST SP800-30, and NERC CIP to support risk understanding, monitoring, and management (Drummond and Machado, 2021; Gunes, Kayisoglu and Bolat, 2021). Another model, the Maritime Cyber Assessment Organization (MCAO), focuses on port operations and critical infrastructure, evaluating regulatory structures and proposing a holistic public–private assessment approach to establish and enforce cybersecurity standards (Trimble, Monken and Sand, 2017).

2.2 Literature about Experts' Perspectives for Improving Regulations

These studies have expert contribute to the academic dialogue on current regulations focus on non-binding guidelines and the subjective interpretation of instruments, aiming to develop better, more robust, and specialized frameworks (Ogundare and Akinwande, 2021; Karim, 2022). Their aim is to foster the development of more robust and specialized frameworks. A significant body of literature advocates for the creation of a standalone cyber code by the IMO to improve legal binding, harmonization, and enforcement, as well as enhance

clarity and modernization (Hopcraft and Martin, 2018; Ogundare and Akinwande, 2021). At the same time, some studies propose focusing on strengthening the existing frameworks and codes. The suggestions include improving the clarity, highlighting the need to strengthen the ISM Code, enhancing clarity and deterrence, and promoting multi-level cooperation and technical customization, as seen in the case of the IACS UR E26 framework, which requires enhancements to a unique environment for ships (Ogundare and Akinwande, 2021; Karim, 2022; Dimakopoulou and Rantos, 2024).

Simultaneously, some studies suggest different tools for standardizing organizational and methodological measures for training and educating personnel. These approaches focus on reducing human error in cybersecurity by suggesting minimum standards. These studies suggest improving quantitative risk assessment methods by considering both Information Technology (IT) and Operational Technology (OT) systems (Sobiesk, Bennett and Maxwell, 2017; Drazovich, Brew and Wetzel, 2021; Drummond and Machado, 2021; Soner *et al.*, 2024).

The existing literature reveals a gap in systematically incorporating stakeholder expert opinions and objectively validating these perspectives. In this study, a total of 38 experts were identified using a Network-Referral-Based method (own pre-existing network), Chain Referral Sampling, and Bibliographic and patent social network analysis. The panels of experts were adequately balanced among representatives from industry, academia, government, and NGOs.

3. Methodology

This study employs a qualitative approach, drawing on experts with experience in maritime cybersecurity and a solid understanding of both operational and regulatory issues. The regulatory frameworks mentioned previously were discussed at length during the maritime cybersecurity TRM sessions. The TRM session was attended by 38 experts from institutions across North America and Europe, representing academia, government, and private industry. The TRM project commenced in October 2024 with an initial stakeholder meeting that laid the groundwork for the subsequent two workshops, which systematically addressed all six NIST Cybersecurity Framework functions (Govern, Identify, Protect, Detect, Respond, and Recover). The

TRM was structured into four "swim lanes": Drivers, Capability Gaps, Technology Characteristics, and R&D programs. For this study, information on Drivers and Capability Gaps was used, as they are directly related to the identification of challenges and gaps. In this context, Drivers are considered as factors associated with organizational changes or decisions, including upcoming regulations and standards (Hillegas-Elting *et al.*, 2015).

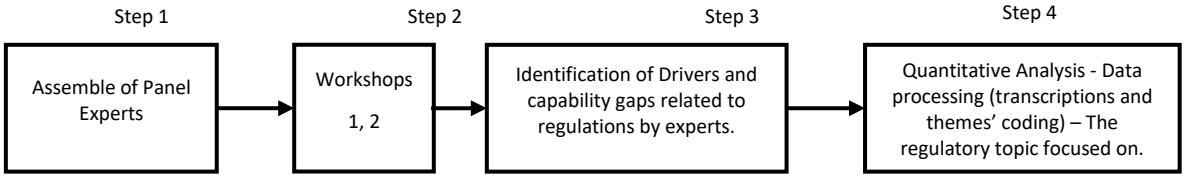

Figure 1: Research Methodology Flow

The process of selecting experts involves identification, contact, engagement, and panel formation. Experts were identified using the Network-Referral-Based method, Chain Referral Sampling, and Bibliographic and patent social network analysis, in accordance with the inclusion criteria of relevant knowledge and experience in maritime cybersecurity, as well as reputation in industry, government, and academia**.** To minimize bias, the selection and invitation of these experts were balanced within each NIST function by expertise type, organizational role, and regional location.

The study utilizes information obtained from two online workshops conducted to develop a technology roadmap. The workshops counted on the participation of 38 experts. These two workshops were organized with distinct objectives, with discussions focusing on technological and regulatory challenges and solutions in maritime cybersecurity. Workshop 1 focused on identifying drivers and capability gaps in the maritime cybersecurity field, with participation from stakeholders, managers, decision-makers, and directors. As mentioned above, the information obtained from this workshop served as a data source for the present study, as it is directly relevant to identifying regulatory challenges. The second workshop focused on technological availability and on new technologies that need to be developed to address the gaps and drivers. The third step involves analytical and qualitative analysis, which includes identifying regulatory challenges and phrases and paragraphs directly related to regulatory elements, thereby coding and grouping them by theme. The data

corresponds to written and audio files. These themes were classified into three categories (governance, people, and technology) based on the type of challenges.

4. Results and Data Analysis

The results of the qualitative analysis from the expert discussions during the two workshops are included in Tables 1, 2, and 3. The process includes three main steps: data transcription, data preparation and standardization, and identification of qualitative components directly related to regulatory topics. These components were organized according to the maritime cybersecurity TRM (Clark *et al.*, 2025) areas and NIST CSF functions. The identified discussions about regulatory challenges were grouped, analyzed by themes, and assigned to their corresponding category. For each theme, similar ideas were merged, and related regulatory references were noted. The analysis also includes identifying the corresponding NIST CSF functions based on panel discussions. Discussions on regulatory challenges were grouped by theme, analyzed, and assigned to their corresponding category. For each theme, similar ideas and opinions were merged, and related regulatory references were noted. Finally, the analysis linked these themes to the appropriate NIST CSF functions based on the panel discussions.

Each table shows the identified regulatory challenges and gaps, categorized into three groups: Governance & Strategy (see Table 1), People & Process (see Table 2), and Technology & Implementation (see Table 3). Each category contains subcategories that explain the challenges and needs associated with it, the type of norms it encompasses, the kinds of security policies it belongs to, and the NIST CSF function associated with the topic. This last aspect was included to maintain the data logically categorized within the context in which the technology roadmap was developed, considering the NIST CSF functions as the roadmap areas.

Table 1: Governance & Strategy (Category 1)

Subcategory	Challenges and Needs	Type of Regulation or Standard, or Framework Referred to	NIST Function
Budgeting and Resource Allocation Gaps	Budget constraints and inconsistent funding impact upgrades and system innovation. The effects include under-prioritized cybersecurity efforts. C-suite executives often have only the minimum required for compliance, related to the high costs of complex systems (integration of IT/OT systems).	IMO requirement (risk management) Regulations (general) R&D Funding	Identify Govern Detect Protect
Regulatory Structure and Clarity (Jurisdiction/Vision) Gaps	The regulatory governance structure and jurisdiction are fragmented and unclear. The results include having undefined cybersecurity enforcement responsibilities. The causes of these issues are related to the lack of a single authority, inconsistent governance, and challenges in implementing a unified risk strategy due to disagreements on core definitions.	ISO Risk Management Strategy	Identify Govern
Standards Development & Maintenance Gaps	Current IACS standards, such as E26/E27, are not effectively enforced on in-service vessels. Additionally, unclear rules and slow regulatory updates affect the responses to attacks. There is a lack of a unified certification framework for IT/OT/IoT devices, and integrating cybersecurity into the ISPS Code is a slow process. It is needed more dynamic standards' ecosystems, as well as more specific and authoritative standards.	IACS Standards (E26, E27) Certification and Accreditation Framework/Authority Regulations and Standards International Ship and Port Facility Security (ISPS) Code framework	Protect Detect Identify
Third-Party/Vendor Risk Management Gaps	External partners or vendors involved in maritime operations often lack awareness of regulatory requirements and formal certification programs, resulting in compliance and security gaps. The decision-making process is weak, where vendors are rarely included in the plans. These plans do not include all the stakeholders, and instead, they are driven by other factors, such as required insurance. The strategic plans should include vendors, regulators, and operators.	Certification Programs Risk Management Platforms Cyber Security Insurance Policies - Institute Cyber Attack Exclusion Clause (CL 380)	Protect Identify Recover Govern

Subcategory	Challenges and Needs	Type of Regulation or Standard, or Framework Referred to	NIST Function
Weak Cybersecurity Governance and Strategy Gaps	Executive leadership often does not treat cybersecurity as a critical business priority. As a result, organizations allocate insufficient funds and hire few personnel. The effects of these practices include excessive pressure on personnel, which can lead to an increase in human errors and the implementation of frameworks poorly. To solve these problems, it is necessary to have proper funding, clear strategic guidance, and ensure that cybersecurity measures are coordinated among all the actors.	Cyber Risk Management Risk Management Framework	Identify Govern

Table 2: People & Process (Category 2)

Subcategory	Challenges and Needs	Type of Regulation or Standard, or Framework Referred to	NIST Function
Compliance Culture and Minimum Requirements Gap	Maritime organizations often undervalue cybersecurity, resulting in compliance with the minimum mandatory requirements, which weakens the system's capacity for resilience.	NIST 2.0 International Association of Classification Societies (IACS) requirements Mandatory Certification Class Certification (Class Societies) IMO requirements and guidelines Vetting Requirements (Ship Inspection Report Programme - SIRE, Chemical Distribution Institute - CDI ship, RightShip) Compliance Regulatory Audits	Identify Protect Detect Govern Recover
Expertise, Training, and Awareness Gap	Maritime organizations frequently face a shortage of personnel with advanced cybersecurity expertise in regulatory awareness, particularly among inspectors and senior leaders. These inconsistent onboarding issues make it difficult for organizations to implement cybersecurity strategies effectively. In addition to having an adequate number of personnel, it is necessary to implement role-specific training programs, standardized training, and have a solid understanding of evolving requirements.	Certification and Training Programs IMO standards and regulations Cybersecurity readiness assessment	Detect Respond Protect Identify Recover Govern
Incident Response and Business Continuity Gap	The regulatory entities offer limited guidance and inconsistent reporting procedures, as maritime organizations often lack comprehensive cybersecurity business continuity plans, standardized drills, and coordinated incident response procedures. Therefore, a unified framework and proactive preparedness are crucial to enhancing resilience across the sector.	Incident Response - IR Planning Cybersecurity Drills and Simulations Safety Management System (SMS), Ship Security Plan (SSP), Ship Security Assessment (SSA) Business Continuity Plans (BCPs)	Respond
Procedure and Documentation Gap	Ports and maritime organizations often lack standardized incident procedures. Organizations generally have inconsistent reporting and outdated recovery guidelines that are poorly integrated into formal documentation. There are inadequate audits, shared policy templates, and uniform documentation practices, which negatively impact strategic planning and communication. A centralized, updated framework is needed to support consistent and effective cyber incident response.	ISM code SMS (Safety Management System) Post Response Reporting Procedures Incident procedures Audits, Procedures Cyber Policy Templates Recovery Guidelines	Respond Identify Recover

Table 3: Technology & Implementation (Category 3)

Subcategory	Challenges or Needs Related to the Standard/Regulation/Frameworks	Type of Regulation or Standard, or Framework Referred to	NIST Function
Asset Management and Inventory Gap	Maritime operations often lack complete asset documentation, onboard cybersecurity ownership, and limited visibility into system vulnerabilities and threats. This implies having untrained personnel for managing critical systems and poorly tracked supply chain risks (embedded modems in port equipment).	Asset Documentation Cybersecurity Ownership IT/OT Asset Identification	Identify
Design, Technology, and Legacy System Integration Gap	Legacy ship systems were not designed for modern cybersecurity technologies, facing challenges in integrating new technologies (e.g., Zero Trust or SIEM). This aspect is associated with system designs and updates. The organizations also lack a consistent evaluation of IoT frameworks and flexible R&D alignment with standards, despite guidance such as IACS UR E26. Therefore, a strategic approach is warranted to bridge design limitations and changes in technological dynamics.	Zero Trust model Security Information and Event Management - SIEM (frameworks/tools) NIST SP800-213 and 213A (IoT frameworks) International Association of Classification Societies (IACS) Unified Requirement UR E26 guidelines Network Standards Series of international standards for the cybersecurity of industrial automation and control systems, IEC 62443 (International Electrotechnical Commission) NIST CSF International Organization for Standardization - ISO 27001 standards	Respond Detect Protect Identify
Implementation & Enforcement Gap	Maritime cybersecurity remains vulnerable to weak enforcement, high compliance costs (meeting cybersecurity requirements often involves expensive upgrades, audits, and certifications), and slow integration into formal systems such as Safety Management Systems (SMS) or International Safety Management (ISM). Stronger regulatory mechanisms, more precise guidance, and streamlined implementation are needed to close the gap between policy and practice.	International Safety Management - ISM code SMS (Safety Management System) Procedures Ship Security Plan - SSP Ship Security Assessment - SSA Class approval IACS Standards (E26, E27) Audits, Procedures Vetting programs	Identify Detect Protect Respond Recover Govern
Security Monitoring and Detection Gap	Older maritime systems lack event monitoring and standardized tools (i.e., SIEM) to detect anomalies in real time. Furthermore, there exists poor threat intelligence sharing across fleets and organizations, reliance on outdated software, and vendor reluctance to report vulnerabilities to protect their reputations. Clear guidelines, built-in security design, and maritime-specific monitoring frameworks are warranted.	Security Event Monitoring Security Information and Event Management - SIEM Security Operations Center - SOC Regulatory Guidelines Mandatory Reporting Requirements	Detect Identify Govern
Vulnerability and Patch Management Gap	Vulnerability management in maritime systems is influenced by legacy OT environments, a lack of built-in software security, and vendor reluctance to disclose flaws due to certification risks. The absence of proactive strengthening strategies and industry-wide debate on secure software design due to the risk that software could be developed without secure coding	Class Certification (Class Societies) Software Quality Requirements	Detect Protect

Subcategory	Challenges or Needs Related to the Standard/Regulation/Frameworks	Type of Regulation or Standard, or Framework Referred to	NIST Function
	practices, leaving it exposed to common vulnerabilities.		

5. Analysis

The results suggest that maritime cybersecurity challenges are linked to fragmented regulatory structures, because maritime cybersecurity rules come from multiple organizations (IMO, flag states, classification societies) and they are not harmonized. Therefore, although regulations exist, enforcement varies by region and authority, resulting in inconsistent enforcement, including minimal compliance and a tendency to maintain outdated infrastructure.

The policies most commonly referenced throughout the study are consistent with established standards, procedures, and frameworks, highlighting a necessity for more structured and adaptable controls. Each subcategory within the three primary categories corresponds to various NIST Cybersecurity Framework (CSF) functions; in fact, all CSF functions are accounted for in this mapping. This alignment is anticipated, as the NIST functions encompass all stages of an organization's cybersecurity lifecycle.

The challenges found within category 1, Governance and Strategy (G), encompass a range of issues, from economic and financial concerns to the structure, development, update, and governance of norms aw well as problems stemming from fragmented organizational structures. Budgeting and resource allocation gaps include compliance requirements and the under-prioritization of cybersecurity efforts. The regulatory structure, with its lack of clarity, is associated with fragmented governance and unclear lines of responsibility. These deficiencies affect the development and maintenance of standards such as E26/E27, which are perceived as insufficiently enforced. Overall, governance and strategy appear fragmented due to limited executive support, the absence of a unified strategy, and the lack of a cohesive certification framework. Weak governance is a cross-cutting issue affecting all topic categories and the risk management process, ultimately hindering the effective implementation of norms.

In the People and Process (P) category, challenges relate to human factors and organizational practices, including gaps in organizational procedures and competencies, operational responses, and documentation. While the causes of this vary, a common theme is that organizations often settle for minimal compliance, which limits the adoption of new protective technologies and adequate personnel training. Other contributing factors include a lack of cyber expertise, standardized training, and regulatory awareness across all organizational levels. These human-centered challenges are linked to a limited understanding of diverse requirements and insufficient onboarding or in-service training. Operational response and documentation issues further indicate the absence of consistent cybersecurity business plans and coordinated response mechanisms across maritime organizations. In this context, establishing standardized incident procedures and maintaining up-to-date policy and guideline libraries is essential.

The last category, Technology & Implementation (T), focuses on technical systems and their deployment. The subcategories address challenges in system infrastructure, design flaws, operational monitoring, and enforcement gaps. A sequential set of issues emerges across asset management, system design, legacy system integration, and vulnerability or patch management. Weak assessments in these areas hinder the effective integration of modern systems into legacy or complex infrastructures, resulting in unmanaged vulnerabilities. Operational monitoring and enforcement gaps include shortcomings in implementing and enforcing existing regulations, particularly those related to the ISM Code and IACS standards. Additionally, security monitoring and detection systems remain inadequate because they rely on outdated tools (e.g., GPS/AIS spoofing detection) and suffer from insufficient information-sharing practices.

6. Conclusion

This paper identified, categorized, and analyzed challenges and gaps within the maritime cybersecurity regulatory framework. Using a qualitative approach, the study draws on insights from 38 subject-matter experts. During two online workshops, experts discussed drivers and capability gaps related to maritime cybersecurity, including regulatory issues. Identified challenges were classified into three categories: governance and strategy, people and processes, and technology and implementation.

The study evaluated Governance & Strategy (G), People & Process (P), and Technology & Implementation (T), encompassing fourteen subcategories addressing key aspects of maritime cybersecurity. Analysis of these categories and recurring challenges reveals systemic gaps, particularly a fragmented regulatory framework combined with weak enforcement, minimal compliance, and unclear norms. This culture of minimal compliance negatively affects operational security. In addition, shortcomings in human capital, expertise development, training, and awareness are linked to insufficient standardized procedures and documentation.

Human-related challenges are critical to fostering stronger compliance cultures, ensuring sufficient expertise, and maintaining properly documented systems. Technological issues are closely connected, as many systems rely on outdated installations that cannot readily integrate modern cybersecurity protections. Legacy technologies pose significant risks because they were not designed to meet contemporary cybersecurity requirements. Even when upgrades occur, poor planning and inadequate standards often lead to incomplete or ineffective controls. Weak assessment management of legacy systems further limits integration of modern security tools, exposing management gaps and undermining security monitoring and enforcement. As a result, regulatory mechanisms fall short of supporting effective operational protection.

This analysis is based on expert perspectives, which introduces subjectivity but is essential for understanding regulatory application in practice. Future studies incorporating academic literature could strengthen the analysis and validate findings across complementary data sources.

References

Amin, M. (2024) "The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets," *Indian Journal of Public Administration*, 70(3), pp. 493–501. Available at: https://doi.org/10.1177/00195561241271520.

Amro, A. and Gkioulos, V. (2023) "Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth," *International Journal of Information Security*, 22(1), pp. 249–288. Available at: https://doi.org/10.1007/s10207-022-00638-y.

Anchore (2025) *Your Guide to Cybersecurity Compliance, from Federal Policy to Industry Standards*. Available at: https://anchore.com/compliance/ (Accessed: November 9, 2025).

Chupkemi, D.C. and Mersinas, K. (2024) "Challenges in Maritime Cybersecurity Training and Compliance," *Journal of Marine Science and Engineering*, 12(10). Available at: https://doi.org/10.3390/jmse12101844.

Clark, U. *et al.* (2025) "Maritime Transportation System (MTS) Cybersecurity Technology Roadmap (TRM) Version 1." Available at: https://hdl.handle.net/20.500.14481/1433 (Accessed: November 16, 2025).

Dimakopoulou, A. and Rantos, K. (2024) "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0," *Journal of Marine Science and Engineering*, 12(6). Available at: https://doi.org/10.3390/jmse12060919.

Djebbar, F. and Nordstrom, K. (2023) "A Comparative Analysis of Industrial Cybersecurity Standards," *IEEE Access*, 11, pp. 85315–85332. Available at: https://doi.org/10.1109/ACCESS.2023.3303205.

Drazovich, L., Brew, L. and Wetzel, S. (2021) "Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system," in *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*. Institute of Electrical and Electronics Engineers Inc., pp. 503–509. Available at: https://doi.org/10.1109/CSR51186.2021.9527922.

Drummond, B.M. and Machado, R.C.S. (2021) "Cyber Security Risk Management for Ports - A Systematic Literature Review," in *2021 IEEE International Workshop on Metrology for the Sea: Learning to Measure Sea Health Parameters, MetroSea 2021 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., pp. 406–411. Available at: https://doi.org/10.1109/MetroSea52177.2021.9611569.

Folorunso, A., Wada, I., *et al.* (2024) "Security compliance and its implication for cybersecurity," *https://wjarr.com/sites/default/files/WJARR-2024-3170.pdf*, 24(1), pp. 2105–2121. Available at: https://doi.org/10.30574/WJARR.2024.24.1.3170.

Folorunso, A., Mohammed, V., *et al.* (2024) "The impact of ISO security standards on enhancing cybersecurity posture in organizations," *https://wjarr.com/sites/default/files/WJARR-2024-3169.pdf*, 24(1), pp. 2582–2595. Available at: https://doi.org/10.30574/WJARR.2024.24.1.3169.

Gunes, B., Kayisoglu, G. and Bolat, P. (2021) "Cyber security risk assessment for seaports: A case study of a container port," *Computers & Security*, 103, p. 102196. Available at: https://doi.org/10.1016/J.COSE.2021.102196.

Heckman, M.R. *et al.* (2017) "Chapter 32: Toward a Maritime Cyber Security Compliance Regime," in J. Direnzo III, N.K. Drumhiller, and F.S. Roberts (eds.) *Issues in Maritime Cyber Security*. Washington DC: Westphalia Press, pp. 543–568.

Hillegas-Elting, J. V. *et al.* (2015) "Opening the door to breakthroughs that address strategic organizational needs: Applying technology roadmapping tools and techniques at an electric utility," *Portland International Conference on Management of Engineering and Technology*, 2015-September, pp. 2564–2573. Available at: https://doi.org/10.1109/PICMET.2015.7273034.

Hopcraft, R. and Martin, K.M. (2018) "Effective maritime cybersecurity regulation–the case for a cyber code," *Journal of the Indian Ocean Region*, 14(3), pp. 354–366. Available at: https://doi.org/10.1080/19480881.2018.1519056.

International Association of Classification Societies IACS (2022a) *UR E26 REV1 -2023 Cyber Resilience of Ships*, *E26*. E26. Available at: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e26-new (Accessed: November 22, 2025).

International Association of Classification Societies IACS (2022b) *UR E27 Rev1 2023 - Cyber Resilience of onboard Systems and Equipment*, *E27*. 2022. Available at: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1 (Accessed: November 22, 2025).

Karim, M.S. (2022) "Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?," *Marine Policy*, 143. Available at: https://doi.org/10.1016/j.marpol.2022.105138.

Ko, A., Lee, J.H. and Seo, J.T. (2025) "KPI-Based Evaluation Framework for Cyber Resilience of Ships," *IEEE Access*, 13, pp. 64226–64245. Available at: https://doi.org/10.1109/ACCESS.2025.3550501.

Melnyk, O., Drozdov, O. and Kuznichenko, S. (2025) "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures," *Lex Portus*, 11(1), pp. 7–19. Available at: https://doi.org/10.62821/lp11101.

Miller, A. (2024) *Tailoring Cybersecurity Measures for Different Industries - AgileBlue*. Available at: https://agileblue.com/resource/tailoring-cybersecurity-measures-for-different-industries-2/ (Accessed: November 9, 2025).

Ogundare, B. and Akinwande, G. (2021) "International Maritime Organisation Framework on Cyber Risk Management-a Case for a Comprehensive Legal Framework." Available at: www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-se-.

Olney, M. (2023) *What are the benefits of cyber security compliance and the consequences of non-compliance?* Available at: https://insights.integrity360.com/what-are-the-benefits-of-cyber-security-compliance-and-the-consequences-of-non-compliance (Accessed: November 9, 2025).

Park, C. *et al.* (2023) "A BN driven FMEA approach to assess maritime cybersecurity risks," *Ocean & Coastal Management*, 235, p. 106480. Available at: https://doi.org/10.1016/J.OCECOAMAN.2023.106480.

Sobiesk, Edward., Bennett, Daniel. and Maxwell, Paul. (2017) "2A Framework for Cybersecurity Assessments of Critical Port Infrastructure," in *2017 IEEE International Conference on Cyber Conflict (CyCon U.S.) : proceedings : 7-8 November 2017, Washington, DC, USA*. IEEE, p. IEEE.

Soner, O. *et al.* (2024) "Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks," *Applied Ocean Research*, 142. Available at: https://doi.org/10.1016/j.apor.2023.103855.

Svilicic, B. *et al.* (2019) "Assessing ship cyber risks: a framework and case study of ECDIS security," *WMU Journal of Maritime Affairs*, 18(3), pp. 509–520. Available at: https://doi.org/10.1007/s13437-019-00183-x.

Taherdoost, H. (2022) "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics 2022, Vol. 11,* 11(14). Available at: https://doi.org/10.3390/ELECTRONICS11142181.

Tam, K. and Jones, K. (2019) "MaCRA: a model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, 18(1), pp. 129–163. Available at: https://doi.org/10.1007/s13437-019-00162-2.

Trimble, D., Monken, J. and Sand, A.F.L. (2017) "A Framework for Cybersecurity Assessments of Critical Port Infrastructure," in Edward. Sobiesk, Daniel. Bennett, and Paul. Maxwell (eds.) *2017 IEEE International Conference on Cyber Conflict (CyCon U.S.) : proceedings : 7-8 November 2017, Washington, DC, USA*. New York City, USA: IEEE.

Wu, Z. *et al.* (2023) "An attack-aware shipping enterprise cybersecurity framework based on deep learning," in *Proceedings - 2023 11th International Conference on Information Systems and Computing Technology, ISCTech 2023*. Institute of Electrical and Electronics Engineers Inc., pp. 115–119. Available at: https://doi.org/10.1109/ISCTech60480.2023.00028