Cyber Risk Management in the Maritime Sector: Implementation of IMO Resolution MSC.428(98) and MSC-FAL.1/Circ.3

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*— The International Maritime Organization (IMO) Resolution MSC.428(98) requires that cyber risks be addressed in the safety management systems (SMS) of shipping companies under the International Safety Management (ISM) Code, supported by the Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3. Several years after the 2021 verification deadline, implementation remains uneven, verification practices differ between flag and port States, and the regime is being reshaped by the 2025 revision of the Guidelines, mandatory classification requirements for new ships, and national rules. This study aims to analyze how the two IMO instruments are translated into company and shipboard practice and to propose a model that strengthens their implementation. A qualitative regulatory implementation analysis was conducted on 15 primary instruments issued between 2017 and 2025 by IMO, flag Administrations, classification societies, port State control regimes, and industry bodies, complemented by a structured review of peer-reviewed studies. The twelve elements of the ISM Code were mapped to the six functional elements of the revised Guidelines using a three-level relevance scale. The results show that governance, identification, and protection are well anchored in existing SMS clauses, whereas detection has only one primary anchor, the reporting of non-conformities, which makes SMS-based cyber risk management largely reactive. Verification also relies on periodic audits rather than technical testing. The study proposes an SMS-integrated cyber risk management model with an audit evidence matrix and a five-stage implementation depth scale, and derives implications for Indonesia. Further research should validate the model with shipping companies and auditors.**

***Keywords*— Maritime cyber risk management; MSC.428(98); MSC-FAL.1/Circ.3; ISM Code; safety management system; port State control.**

Manuscript received xx xxx. 2026; revised xx xxx. 2026; accepted xx xxx. 2026. Date of publication xx xxx. 2026.
International Journal on Informatics Visualization is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. INTRODUCTION

Ships have become floating networks. Navigation, propulsion, cargo handling, ballast control, and communication increasingly depend on computer-based systems that are interconnected with one another and with shore-based offices, equipment vendors, and satellite links. This convergence of information technology (IT) and operational technology (OT) improves efficiency but exposes safety-critical functions to cyber threats [1], [2]. Experimental assessments have demonstrated exploitable vulnerabilities in shipboard Electronic Chart Display and Information Systems (ECDIS) and radars [3], [4], and risk analyses of ship systems show that cyber-attacks on engines and automation can produce consequences comparable to those of conventional technical failures [5], [6]. Retrospective analyses confirm that cyber incidents affecting ships and shipping companies are neither hypothetical nor rare [7], [8].

The International Maritime Organization (IMO) responded with two complementary instruments. The Guidelines on Maritime Cyber Risk Management, issued as MSC-FAL.1/Circ.3 in 2017, provide high-level recommendations and functional elements for managing cyber risk [9]. Resolution MSC.428(98), adopted on 16 June 2017, affirms that an approved safety management system (SMS) should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code, and encourages Administrations to ensure that cyber risks are appropriately addressed no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021 [10]. By anchoring cyber risk in the ISM Code, which is mandatory under SOLAS chapter IX [11], IMO chose to treat cyber risk as a safety management issue rather than to create a separate convention.

This regulatory design has strengths and weaknesses. It leverages an established, audited management system and avoids new treaty obligations, but it leaves the content of compliance largely to companies, flag Administrations, and their recognized organizations. Classification societies announced that compliance would be verified by ISM auditors at ship and shore-based audits from 1 January 2021 [12], and some port States signalled strict enforcement, including detention of ships whose SMS had not incorporated cyber risk management [13]. Other regimes, by contrast, emphasize that ISM auditing remains the responsibility of the flag State and the company and lies outside the scope of port State control (PSC) [14]. The regime has also continued to evolve: the Guidelines were revised in 2022 and again in April 2025, when a Govern function was added [15], [16]; the unified requirements UR E26 and UR E27 of the International Association of Classification Societies (IACS) became mandatory for ships contracted for construction on or after 1 July 2024 [17], [18]; the United States adopted binding cybersecurity rules for its

flag fleet and facilities [19]; and IMO agreed in 2025 to develop a non-mandatory Cybersecurity Code for ships and port facilities [20].

Existing research has concentrated on threats, vulnerabilities, and risk assessment methods [21], [22], [23], on onboard readiness [24], and on human factors such as cyber risk perception [25]. Reviews note that the maritime cyber literature remains fragmented and that regulatory implementation has received comparatively little systematic attention [26], [27]. Kontovas and Chang recently discussed current and future regulatory compliance approaches and highlighted the inadequate security controls of vulnerable onboard systems [28], but a clause-level analysis of how the ISM Code accommodates the functional elements of the IMO Guidelines, and of the evidence that auditors should expect, is still missing.

The question is also practical for Indonesia, an archipelagic flag and port State whose domestic and international fleets are subject to ISM and ISPS obligations. Indonesian scholars have observed that national maritime cybersecurity policies remain limited [29], although the Directorate General of Sea Transportation issued Circular Letter No. 16 of 2024 on cyber security assessment and procedures in ship and port facility security management [30]. How such national measures relate to the SMS-based approach of MSC.428(98) has not been examined.

This study therefore has three objectives: (1) to analyze the implementation chain through which MSC.428(98) and MSC-FAL.1/Circ.3 are translated into company and shipboard practice; (2) to map the elements of the ISM Code to the functional elements of the revised Guidelines in order to identify where cyber risk management is well anchored and where it is not; and (3) to propose an SMS-integrated implementation model with audit evidence and an implementation depth scale, together with implications for Indonesia. Section II describes the materials and method, Section III presents and discusses the results, and Section IV concludes the paper.

II. MATERIALS AND METHOD

A. Research Design

The study adopted a qualitative regulatory implementation analysis, which examines how a policy instrument is translated through successive actors into organizational practice and how compliance is verified. The design combined document analysis of primary regulatory and quasi-regulatory instruments, a clause-level traceability mapping, and a structured synthesis of peer-reviewed literature. The procedure consisted of five steps, shown in Fig. 1.

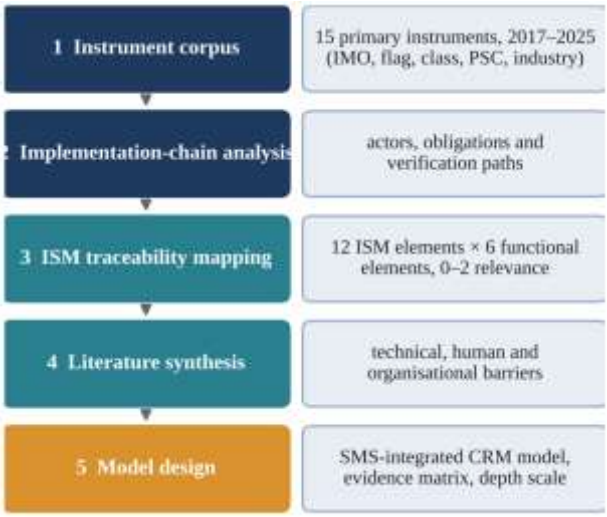


Fig. 1 Research procedure of the regulatory implementation analysis

B. Materials

The primary corpus comprised 15 instruments issued between 2017 and 2025 (Table I). They were selected because they either establish the obligation (IMO), translate it into national requirements or verification practice (flag Administrations, classification societies, and PSC regimes), or provide the operational guidance that companies use to comply (industry guidelines). The ISM Code itself, adopted by resolution A.741(18) as amended [11], served as the reference text for the mapping. NIST CSF 2.0 [31] and ISO/IEC 27001 [32] were consulted as reference frameworks because the IMO functional elements derive from the NIST framework and because some companies choose certified information security management systems.

TABLE I
PRIMARY INSTRUMENTS ANALYSED

Instrument (year)	Issuer and nature	Implementation role
MSC.428(98) (2017)	IMO; resolution	Links cyber risk to SMS; 2021 deadline
MSC-FAL.1/Circ.3 (2017)	IMO; guidelines	Functional elements
MSC.1/Circ.1639 (2021)	IMO; circular	Circulates industry guidelines
MSC-FAL.1/Circ.3/Rev.2 (2022)	IMO; guidelines	Refined guidance
MSC-FAL.1/Circ.3/Rev.3 (2025)	IMO; guidelines	Adds Govern; aligns with CSF 2.0
MSC 110 outcome (2025)	IMO; decision	Non-mandatory Cybersecurity Code
IACS UR E26 Rev.1 (2023)	Class; mandatory	Ship cyber resilience (newbuilds)
IACS UR E27 Rev.1 (2023)	Class; mandatory	Onboard systems and equipment
Guidelines on Cyber Security Onboard Ships v5 (2024)	Industry; guidance	SMS integration, risk assessment
Class news 22/20 (2020)	RO; notice	ISM audits from 2021
USCG work instruction (2020)	Port State; instruction	PSC actions, detention
USCG final rule (2025)	National; regulation	Plans, officer, reporting
Paris MoU PSCC 58/2025/15 (2025)	PSC regime; instruction	ISM outside PSC audit scope
SE Dirjen Hubla No. 16/2024	Flag (Indonesia); circular	ISPS-based cyber procedures
Perpres No. 82/2022	Indonesia; regulation	Transport as vital sector

Secondary materials consisted of peer-reviewed studies on maritime cyber risk published mainly between 2020 and 2025, identified through searches of journal databases and screened for relevance to ship and company level risk management, implementation barriers, and human factors.

C. Traceability Mapping and Indices

The twelve elements of the ISM Code (clause 1.2.2 on risk assessment and safeguards, and sections 2 to 12) were mapped to the six functional elements of MSC-FAL.1/Circ.3/Rev.3: Govern, Identify, Protect, Detect, Respond, and Recover. For each ISM element c and function f, a relevance score $r_{c,f}$ was assigned on a three-level scale: 0 (no meaningful link), 1 (supporting link, where the clause can host the function indirectly), and 2 (primary anchor, where the clause provides a direct and auditable home for the function). The mapping drew on the SMS integration guidance in the industry guidelines [33], which associates, for example, the safety and environmental policy (ISM 2), training (ISM 6.5), critical systems (ISM 10.3), and back-ups with specific cyber measures, and extended this guidance to all elements and to the Govern function introduced in Rev.3.

Two indices were derived for each function. The traceability index expresses the overall strength of links between the ISM Code and the function across all $C = 12$ elements:

$$TI_f = \frac{\sum_{c=1}^{C} r_{c,f}}{2C} \times 100\% \quad (1)$$

The primary anchor count identifies how many ISM elements provide a direct home for the function, where δ denotes the Kronecker delta:

$$PA_f = \sum_{c=1}^{C} \delta(r_{c,f}, 2) \quad (2)$$

A function with a low traceability index or a single primary anchor is weakly embedded in the SMS and is therefore at risk of being treated as a paper requirement during audits.

D. Trustworthiness

Credibility was supported by grounding each mapping decision in the text of the ISM Code and the IMO Guidelines, and by cross-checking against the industry guidance that maps SMS clauses to cyber measures. Dependability was supported by fixing the scoring rules before mapping. Because the scores are interpretive, they are reported transparently in Fig. 4 so that readers can re-examine individual cells.

III. RESULTS AND DISCUSSION

A. Evolution of the Regulatory Regime

Fig. 2 places the instruments on a timeline. Three phases can be distinguished. In the first phase (2016 to 2020), the regime was soft and industry-led: the joint industry Guidelines on Cyber Security Onboard Ships preceded the IMO instruments, and MSC.428(98) and MSC-FAL.1/Circ.3 established the expectation that cyber risk would be integrated into SMS by 2021 [10], [9]. In the second phase (2021 to 2023), the deadline transformed the expectation into an audited requirement. IMO circulated the industry guidelines as MSC.1/Circ.1639 in June 2021 [34], and the 2022 revision of the Guidelines refined their content [15].

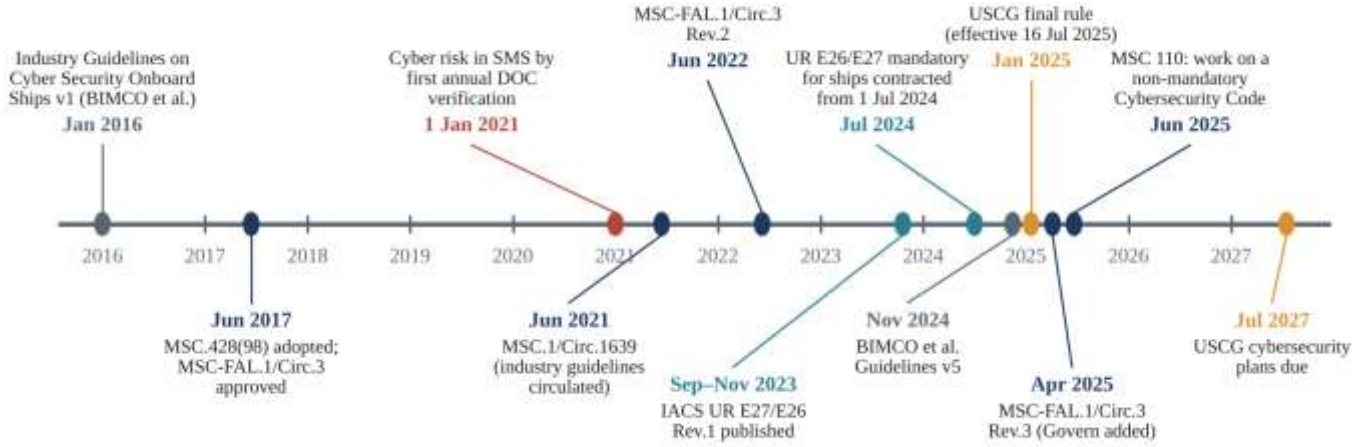


Fig. 2 Timeline of the maritime cyber risk management regime from industry guidelines (2016) to emerging binding and code-based instruments (2027)

The third phase, from 2024 onwards, is marked by hardening and diversification. IACS published Rev.1 of UR E27 in September 2023 and of UR E26 in November 2023, after withdrawing the original 2022 versions before they entered into force, and both became mandatory for ships contracted for construction on or after 1 July 2024 [17], [18]. The fifth version of the industry guidelines, released in November 2024, emphasizes regular updates of cyber risk assessments [33]. The United States Coast Guard published a final rule on 17 January 2025, effective 16 July 2025, which requires a Cybersecurity Officer, a cybersecurity assessment, and an approved Cybersecurity Plan for U.S.-flagged vessels and regulated facilities [19]. At IMO, the 2025 revision of the Guidelines introduced the Govern function [16], and the Maritime Safety Committee agreed at its 110th session to develop a risk-based, non-mandatory Cybersecurity Code covering ships and port facilities [20]. MSC.428(98) thus remains the global baseline, but it now coexists with design-stage class rules and national regulations of a more prescriptive nature.

B. The Implementation Chain

Fig. 3 depicts the chain through which the IMO norm reaches the ship. Because MSC.428(98) operates through the ISM Code, the decisive actors are flag Administrations, which issue national circulars and certify companies and ships, and the recognized organizations that conduct ISM audits on their behalf [12]. Companies translate the obligation into SMS procedures under the authority of the designated person ashore, and masters and crews execute those procedures on board. Classification societies add a second, technical channel through UR E26 and UR E27, which govern the design, integration, and testing of computer-based systems for newbuildings [17], [18].

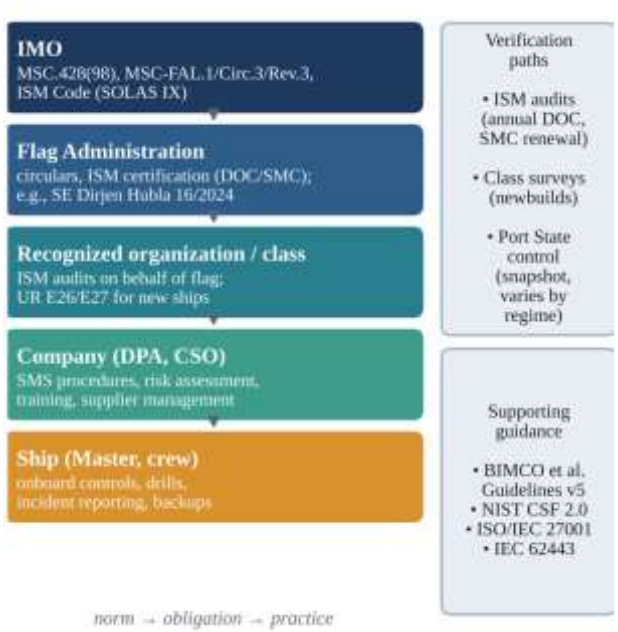


Fig. 3 Implementation chain of MSC.428(98) from IMO to the ship, with verification paths and supporting guidance

The analysis reveals two structural features of this chain. First, verification is heterogeneous. The United States instructed its inspectors to evaluate cyber risk management in the SMS and to consider detention where it had not been incorporated by the first annual DOC verification after 1 January 2021 [13], whereas the Paris MoU instructs its officers that ISM verification is the responsibility of the flag State and the company and does not fall within the scope of PSC [14]. A ship may therefore face very different scrutiny depending on its trading pattern. Second, verification is documentary and periodic. ISM audits sample procedures and records, while PSC inspections provide only a snapshot of a ship on a given day [14]. Neither path routinely tests whether controls work technically, which explains why companies can achieve compliance on paper while vulnerabilities in systems such as ECDIS persist [3], [28].

The chain also shows that companies have flexibility in choosing management frameworks. A German flag guidance note clarifies that a stand-alone ISO/IEC 27001 management system is not required and that integration into the SMS is sufficient, although a certified system can satisfy the IMO expectation if it is integrated with the SMS [35]. This flexibility helps small operators but contributes to variation in implementation quality.

C. ISM Code and Functional Element Traceability

Fig. 4 presents the traceability matrix, and Table II summarizes the indices. Govern is the most strongly embedded function (TI = 50.0%, four primary anchors), because the policy (ISM 2), company responsibilities (ISM 3), the designated person (ISM 4), and verification and review (ISM 12) provide natural homes for cyber policy, roles, and management review. Protect has three primary anchors in resources and personnel (ISM 6), shipboard operations (ISM 7), and maintenance (ISM 10), which can host training, access control, removable media procedures, and patch management. Identify is anchored in the risk assessment requirement of clause 1.2.2 and in the identification of critical equipment and systems under ISM 10.

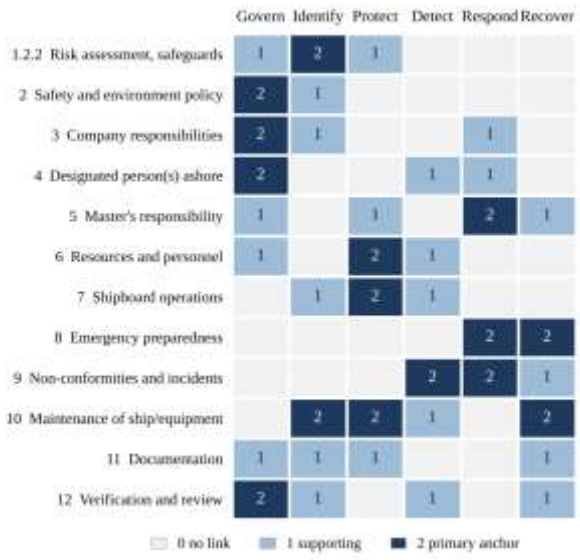


Fig. 4 Traceability matrix between ISM Code elements and the functional elements of MSC-FAL.1/Circ.3/Rev.3 (0 = no link, 1 = supporting, 2 = primary anchor)

TABLE II
TRACEABILITY INDICES PER FUNCTIONAL ELEMENT

Function	TI (%)	PA	Linked elements
Govern	50.0	4	8
Identify	37.5	2	7
Protect	37.5	3	6
Detect	29.2	1	6
Respond	33.3	3	5
Recover	33.3	2	6

Respond and Recover are anchored mainly in emergency preparedness (ISM 8), which requires procedures, drills, and exercises for potential emergency situations. Treating a cyber incident that affects navigation or propulsion as a shipboard emergency allows companies to reuse existing drill regimes, and ISM 10 provides a home for back-ups and restoration of critical systems. The master's overriding authority (ISM 5) is also essential for decisions such as isolating networks or reverting to manual operation.

Detect is the weakest function (TI = 29.2%) and has only one primary anchor: the reporting and analysis of non-conformities, accidents, and hazardous occurrences under ISM 9. This anchor is inherently reactive, because it presupposes that an anomaly has already been noticed by a person. No ISM element requires continuous monitoring of networks or systems, which is consistent with the observation that security monitoring remains an understudied and underdeveloped area in maritime operations [36]. In practice, the detection capability of a ship therefore depends on the technical design of its systems, which is precisely what UR E26 addresses for newbuildings [17]. Existing ships, which make up most of the world fleet and are not retroactively subject to these unified requirements, lack an equivalent design-stage safeguard.

D. Audit Evidence

Because the ISM Code is non-prescriptive, auditors and inspectors need clear expectations regarding the objective evidence that demonstrates effective implementation. Table III proposes an evidence matrix that links each functional element to the ISM clause that hosts it, the documented artefact that should exist, and the record that demonstrates implementation. The matrix distinguishes documents, which show that a procedure exists, from records, which show that it is applied. This distinction addresses the risk of paper compliance identified above and gives flag Administrations and recognized organizations a consistent basis for grading findings.

TABLE III
AUDIT EVIDENCE MATRIX FOR SMS-BASED CYBER RISK MANAGEMENT

Function	ISM	Document	Record
Govern	2, 3, 4, 12	Cyber policy; roles of DPA and cyber focal point	Management review minutes covering cyber
Identify	1.2.2, 10	IT/OT inventory; ship-specific risk assessment	Dated, reviewed assessment; updates after changes
Protect	6, 7, 10	Access, removable media, patch and remote access procedures	Training logs; patch and access records
Detect	9, 10	Definition of cyber hazardous occurrences; monitoring settings	Incident and near-miss reports; alarm or log reviews
Respond	5, 8	Cyber incident response plan; contacts	Drill reports including cyber scenarios
Recover	8, 10	Backup and restoration procedure; manual modes	Backup tests; restoration drill records

E. Implementation Barriers

The literature and the instruments point to four groups of barriers, summarized in Table IV. Technical barriers stem from legacy OT with long life cycles, limited patchability,

and vendor-controlled remote access; experimental assessments of ECDIS and radar illustrate how such systems can remain vulnerable throughout their service life [3], [4]. Human barriers include limited cyber awareness among seafarers and risk perceptions shaped by experience and organizational context [25], [24]; maritime education has been slow to integrate cybersecurity competencies [27]. Organizational barriers include constrained resources in small and medium-sized companies and the fragmentation of guidance across IMO, class, industry, and national regimes, which complicates compliance [28], [23]. Regulatory barriers arise from the non-prescriptive character of MSC.428(98) and from heterogeneous verification across flag and port States [14], [13].

TABLE IV
IMPLEMENTATION BARRIERS AND MITIGATION

Barrier	Manifestation	Mitigation
Technical	Legacy OT, limited patching, vendor remote access	Supplier requirements based on UR E27; segregation; controlled remote access
Human	Low awareness; varied risk perception	Role-based training; cyber drills; reporting culture
Organizational	Limited resources; fragmented guidance	Fleet-level templates; shared services; single SMS reference
Regulatory	Non-prescriptive rule; uneven verification	Evidence matrix; harmonized flag guidance; auditor training

F. SMS-Integrated Cyber Risk Management Model

Building on these findings, the study proposes an SMS-integrated cyber risk management model (Fig. 5). The model places the six functional elements inside the plan-do-check-act logic that the ISM Code already embodies. Planning draws on risk assessment (ISM 1.2.2), policy (ISM 2), and responsibilities (ISM 3); doing relies on resources and training (ISM 6), shipboard operations (ISM 7), and maintenance (ISM 10); checking uses non-conformity reporting (ISM 9) and internal audits and management review (ISM 12); and acting closes the loop through corrective action and emergency preparedness (ISM 8 and 12). Each functional element is linked to concrete artefacts that form the audit evidence of Table III.

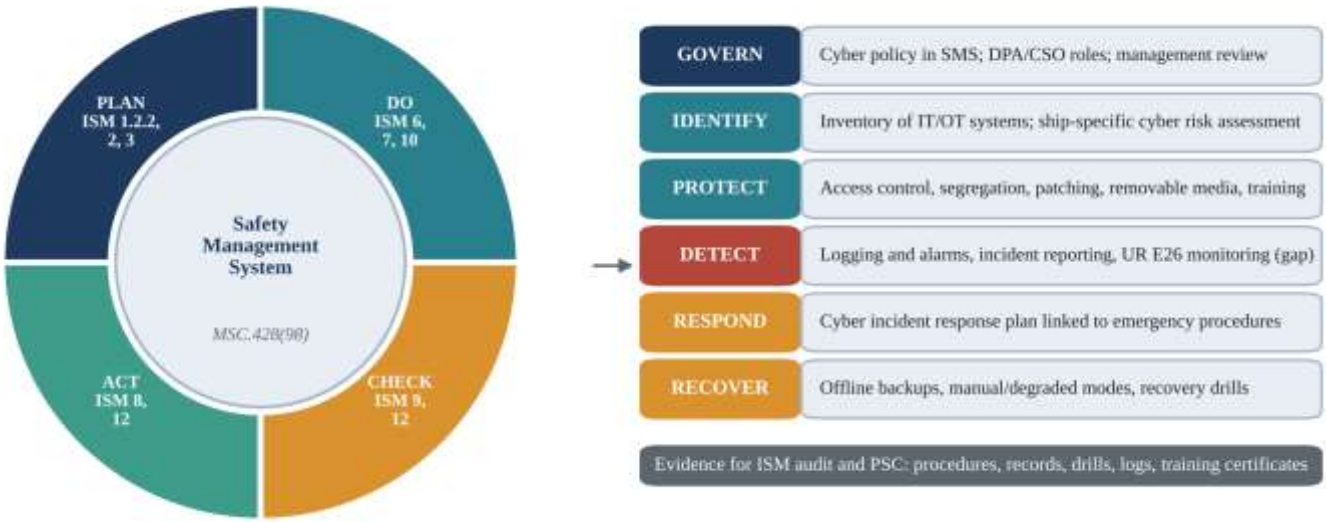


Fig. 5 SMS-integrated cyber risk management model linking the ISM plan-do-check-act cycle to the functional elements of MSC-FAL.1/Circ.3/Rev.3

Two features distinguish the model from a purely documentary approach. First, it treats Detect as an explicit design target. Companies are encouraged to specify logging, alarm, and monitoring capabilities when procuring or upgrading systems, using UR E26 and UR E27 as reference requirements even for existing ships [17], [18], and to define cyber-related hazardous occurrences that crews must report under ISM 9. Second, it measures implementation depth rather than mere presence. Five stages are defined: Stage 0 (absent), in which cyber risk is not addressed in the SMS; Stage 1 (documented), in which a policy and procedures exist; Stage 2 (implemented), in which records show that controls, training, and drills are applied; Stage 3 (verified), in which internal audits and technical tests confirm effectiveness; and Stage 4 (adaptive), in which incident and threat information drives continuous improvement of the SMS. Stage 1 corresponds to the minimum that may pass a documentary audit, whereas the intent of MSC.428(98), safe shipping that is operationally resilient to cyber risks [10], is only achieved from Stage 3 onwards.

G. Implications for Indonesia

Three implications follow for Indonesia. First, Circular Letter No. 16 of 2024 is framed around cyber security

assessment and procedures in ship and port facility security management, that is, around the ISPS Code [30], whereas MSC.428(98) operates through the ISM Code and the SMS. Indonesian companies may therefore face two parallel cyber requirements, one in the ship security plan and one in the SMS. A harmonized national guidance that cross-references both, using the evidence matrix of Table III, would reduce duplication and help auditors grade findings consistently. Second, because maritime transportation is a vital information infrastructure sector under Presidential Regulation No. 82 of 2022 [37], companies operating critical domestic routes could be required to reach at least Stage 2 of the implementation depth scale, with sector coordination involving the Ministry of Transportation and the National Cyber and Crypto Agency. Third, the human barrier calls for capacity building. Maritime academies and polytechnics can integrate shipboard cyber hygiene, incident reporting, and cyber drills into training programmes, and Indonesian research on maritime cyber policy [29] can be extended to empirical assessments of SMS implementation in national fleets.

H. Limitations

This study is based on document analysis and an interpretive mapping; it does not include audit data, PSC deficiency statistics, or interviews with companies and auditors. The relevance scores in Fig. 4 reflect the authors' judgment, although they are reported transparently. The regime is evolving rapidly, and the forthcoming IMO Cybersecurity Code may change the relationship between the ISM Code and cyber risk management. These limitations define the agenda for further empirical work.

IV. CONCLUSION

This study analyzed how IMO Resolution MSC.428(98) and the Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, are implemented through the ISM Code. The implementation chain shows that the regime relies on flag Administrations, recognized organizations, and companies to define the content of compliance, and that verification by ISM audit and port State control is heterogeneous, documentary, and periodic. The traceability analysis shows that Govern, Identify, and Protect are well anchored in existing SMS clauses, whereas Detect has only one reactive primary anchor in non-conformity reporting and is the weakest function (TI = 29.2%). Implementation barriers are technical, human, organizational, and regulatory.

The proposed SMS-integrated cyber risk management model, together with the audit evidence matrix and the five-stage implementation depth scale, offers companies, auditors, and Administrations a practical route from documentary compliance to verified resilience. For Indonesia, harmonizing the ISPS-oriented Circular Letter No. 16 of 2024 with the SMS-based approach of MSC.428(98) is a priority. Further research should validate the model through case studies with shipping companies, analysis of audit and PSC findings, and expert panels, and should examine how the forthcoming IMO Cybersecurity Code will interact with the ISM Code.

ACKNOWLEDGMENT

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

REFERENCES

[1] 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.

[2] 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.

[3] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *J. Navig.*, vol. 72, no. 5, pp. 1108–1120, 2019, doi: 10.1017/S0373463318001157.

[4] B. Svilicic, I. Rudan, V. Frančić, and D. Mohović, "Towards a cyber secure shipboard radar," *J. Navig.*, vol. 73, pp. 547–558, 2020, doi: 10.1017/S0373463319000808.

[5] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Saf. Sci.*, vol. 131, 2020, Art. no. 104908, doi: 10.1016/j.ssci.2020.104908.

[6] V. Bolbot *et al.*, "Cybersecurity risk assessment of a marine dual-fuel engine on inland waterways ship," *Proc. Inst. Mech. Eng. M, J. Eng. Marit. Environ.*, 2024, doi: 10.1177/14750902241265173.

[7] 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.

[8] 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.

[9] International Maritime Organization, "Guidelines on maritime cyber risk management," MSC-FAL.1/Circ.3, London, U.K., Jul. 5, 2017.

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

[11] International Maritime Organization, *International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code)*, Resolution A.741(18), as amended, London, U.K.: IMO, 1993.

[12] Lloyd's Register, "Maritime cyber risk management in safety management systems: Class news 22/2020," London, U.K., Dec. 10, 2020. [Online]. Available: https://www.lr.org/en/knowledge/class-news/22-20/

[13] BIMCO. (2020, Nov. 24). *US to impose tough port State control measures on cyber risk management*. [Online]. Available: https://www.bimco.org

[14] Paris Memorandum of Understanding on Port State Control, "Guidelines for the port State control officer on the ISM Code," PSCC Instruction 58/2025/15, The Hague, The Netherlands, 2025.

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

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

[17] International Association of Classification Societies, "Cyber resilience of ships," Unified Requirement E26, Rev.1, London, U.K., Nov. 2023.

[18] International Association of Classification Societies, "Cyber resilience of on-board systems and equipment," Unified Requirement E27, Rev.1, London, U.K., Sep. 2023.

[19] U.S. Coast Guard, "Cybersecurity in the marine transportation system," Final rule, *Fed. Regist.*, vol. 90, no. 11, p. 6298, Jan. 17, 2025.

[20] International Union of Marine Insurance. (2025, Sep.). *Update on the 110th session of the IMO Maritime Safety Committee (MSC 110)*. [Online]. Available: https://iumi.com/newsletter-september-2025/update-on-the-110th-session-of-the-imo-maritime-safety-committee-msc-110/

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[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] 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.

[27] 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.

[28] C. Kontovas and C.-H. Chang, "Maritime cybersecurity risk management: A discussion on current and future regulatory compliance approaches," in *Proc. Int. Assoc. Marit. Econ. (IAME) Conf.*, Bergen, Norway, Jun. 2025.

[29] R. Desiana and S. C. Prima, "Cyber security policy in Indonesian shipping safety," *J. Marit. Stud. Natl. Integr.*, vol. 5, no. 2, 2021, doi: 10.14710/jmsni.v5i2.13673.

[30] ANTARA News Jawa Timur. (2024, Jun. 11). *DJPL Kemenhub ingatkan pentingnya penerapan ISPS Code di TTL* [Directorate General of Sea Transportation stresses ISPS Code implementation at Teluk Lamong Terminal]. [Online]. Available: https://jatim.antaranews.com/berita/793908/djpl-kemenhub-ingatkan-pentingnya-penerapan-isps-code-di-ttl

[31] 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.

[32] *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, ISO/IEC 27001:2022, International Organization for Standardization, Geneva, Switzerland, 2022.

[33] BIMCO *et al.*, "The guidelines on cyber security onboard ships," Version 5, Bagsværd, Denmark, Nov. 14, 2024.

[34] International Maritime Organization, "The guidelines on cyber security onboard ships," MSC.1/Circ.1639, London, U.K., Jun. 14, 2021.

[35] German Flag (BSH). *Do shipping companies have to introduce a stand-alone ISO management system for cyber protection?* [Online]. Available: https://www.deutsche-flagge.de (accessed Nov. 19, 2026).

[36] 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.

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