INTERNATIONAL
MARITIME
ORGANIZATION

MARITIME SAFETY COMMITTEE MSC 111/7
111th session 06 October 2025
Original: ENGLISH
Pre Session Public
Release:☑

A PRAGMATIC FRAMEWORK FOR MARITIME CYBER RESILIENCE: FINAL DIRECTIVE

An Operator-Centric Approach to IMO Rule Development and Compliance

Submitted by Team B3, Indian Maritime University, Kolkata Campus
(W.R.T. Developed Nations - Category B)

1. Executive Summary and Strategic Direction

This document proposes a holistic and pragmatic framework for building maritime cyber resilience, specifically in reference to the discussions held at the **109th and 110th Maritime Safety Committee (MSC) sessions**. The integration of IT and OT (Information and Operational Technology) systems has created a **digital paradox** where threats directly impact safety-critical systems. We assert that a rigid, prescriptive regulatory approach will fail. Our framework advocates for a **flexible, operator-centric approach** centered on a **non-mandatory, goal-based Code**. This plan integrates three pillars—Technology, Process, and People—to ensure the future of maritime trade is both efficient and secure. This proposal provides the action plan and tools required for the IMO's next steps.

2. The Necessity of a Goal-Based Regulatory Paradigm

The threat landscape—spanning navigational system attacks (GPS Spoofing) to shoreside ransomware (Maersk, COSCO)—is complex and rapidly changing. The existing approach of adding "cyber" to the ISM Code is insufficient for this scale and complexity.

- **Relevance for Next IMO Sessions:** Future regulations must address the operational and financial realities faced by global operators. Rigid, prescriptive rules are particularly difficult for our category of nations (e.g., New Zealand, Norway, Denmark, South Korea) which possess modern fleets but may have limited indigenous cybersecurity R&D and trained IT manpower.
- **The Three Pillars of Resilience:** We propose a framework centered on a Goal-Based Code that integrates three essential pillars:

Pillar	Focus	Why a Goal-Based Code Works
TECHNOLOGY	Layered technical defenses and asset management.	Allows operators to select technologies that fit their operational budget and requirements.
PROCESS	Embedding a mandatory, scalable risk management lifecycle.	Provides the high-level framework (e.g., NIST CSF) while allowing flexibility in implementation tools (e.g., GRC vs. MS 365).
PEOPLE	Building a vigilant, security-first culture through specialized training.	Enables the HTW Sub-Committee to develop globally standardized courses tracked by an LMS.

3. Solution 1: The New Code for Maritime Cyber Resilience (Rule Development)

We propose the IMO adopt a new instrument for maritime cybersecurity founded on a **non-mandatory, goal-based approach**.

Blueprint: Adapting the NIST Cybersecurity Framework (CSF) 2.0

The Code's structure should directly adapt the globally respected and technology-neutral **NIST Cybersecurity Framework (CSF) 2.0**. This provides an instant, recognized structure for both implementation and audit compliance.

Code Chapter (NIST Function)	Core Regulatory Goal	Required Compliance Action
1. GOVERN	Integrate cyber risk into the existing Safety Management System (SMS).	Define roles, responsibilities, and a formal policy.
2. IDENTIFY	Create and maintain an inventory of all critical IT and OT assets.	Implement a scalable **Risk Management Process**.
3. PROTECT	Implement safeguards against threats.	Mandate network segmentation (IT/OT separation) and access control.
4. DETECT	Monitor systems to identify potential intrusions.	Implement continuous vessel and shore monitoring objectives.
5. RESPOND	Define requirements for a pre-planned incident response.	Develop scenario-based response plans for kinetic (OT) and logistical (IT) attacks.
6. RECOVER	Goals for restoring systems and learning lessons.	Establish goals for system restoration and business continuity.

4. Solutions 2 & 3: Pillars of Compliance (People & Technology)

4.1. Solution 2: Mandate Tiered Cybersecurity Training (Necessity of Amendments)

The Human Element remains the primary attack vector. To address this, the **HTW Sub-Committee** must develop a standardized curriculum to support new mandatory training.

Tier	Target Personnel	Duration/Depth	Technology for Tracking
Tier 1 (Awareness)	All Seafarers	60-90 minute interactive e-learning.	**Learning Management System (LMS)** using **SCORM** packages for global deployment and certification tracking.
Tier 2 (Officer)	Designated Ship/Port Cybersecurity Officer	3-5 day in-depth course.	LMS-based certification leading to compliance during vessel audits.

4.2. Solution 3: Establish an IMO-Led Threat Sharing Platform

This is a critical technology requirement for global, real-time defense.

Component	Technology/Standard	Rationale for IMO-Led System
Architecture	Secure Web Application (React frontend, Django REST backend, PostgreSQL).	Centralized data processing and necessary anonymization.
Interoperability	**STIX/TAXII Protocol**.	Allows large operators to automatically feed threat intelligence directly into their internal security tools (**SIEMs**).
Legal Framework	Legal Committee must develop a framework to ensure liability protection for those sharing data.	Encourages wider industry participation by mitigating risk.

5. A Pragmatic Implementation Roadmap (2026-2031+)

This phased roadmap ensures the final regulation is informed by practical data, a key factor for the successful transition from voluntary guidelines.

Phase	Timeline	Action/IMO Deliverable
Phase 1	**2026-2027**	**Development of the Non-Mandatory Code.** The MSC drafts and adopts the Goal-Based Code, using NIST CSF 2.0 as the template.
Phase 2	**2028-2030**	**Structured Experience-Building Phase (EBP).** Operators voluntarily implement the Code and report challenges, costs, and benefits to the IMO.
Phase 3	**2031+**	**Development of a Mandatory Instrument.** Using the EBP data, the IMO drafts a fair and practical mandatory regulation, having de-risked the policy process.

6. Conclusion and Call to Action

The consequences of cyber inaction pose a clear and present danger to SOLAS and the global supply chain. The proposed holistic framework, rooted in a flexible, goal-based Code and the three essential pillars, is the only pragmatic and scalable path forward for the maritime industry. We respectfully request that the Maritime Safety Committee:

1. **Rule Development (MSC):** Agree in principle to a new IMO instrument for maritime cybersecurity and establish an output to develop the **Non-Mandatory International Code for Maritime Cyber Resilience**.
2. **Necessity of Amendments (HTW):** Instruct the relevant Sub-Committees to support this work by developing the proposed **tiered IMO Model Courses** to address the persistent human element vulnerability.
3. **Regulatory Compliance (Legal):** Develop the legal framework required for liability protection to support the proposed **Threat Sharing Platform**.

The conclusion must be clearly mentioned: This approach ensures that maritime security is enhanced **pragmatically and scalably**, leading to genuine cyber resilience and protecting the entire digital-ecosystem.