TECHNICAL CIRCULAR No. 849 of 5th November 2024

To	All Surveyors/Auditors. All flags
Title	**MARITIME SECURITY- Cyber Risk Management**
Reference	IMO Guidelines

MARITIME SECURITY

Revision of the Guidelines on Maritime Cyber Risk Management (Msc-Fal.1/Circ.3/Rev.2)

The Committee has approved a revision to the Guidelines on Maritime Cyber Risk Management. The updated circular, MSC-FAL.1/Circ.3/Rev.3, supersedes the interim guidelines in MSC.1/Circ.1526. The revision includes:

• Additional definitions for Computer Based System (CBS), Cyber incident, Information Technology (IT), and Operational technology (OT).

• Expansion of the list of systems critical to the safety and security of shipping and protection of the marine environment to include navigation systems, ship safety systems and communications systems, bunkering, lubrication, ballast, and fuel systems, security, access control and surveillance systems, crew and service personnel management systems, ship-port interfaces; and ship to shore integrated systems (e.g. remote control systems/Maritime Autonomous Surface Ships).

• Functional/technical cybersecurity controls listed under each functional element, representing the minimum controls to be implemented. These controls and functional elements relate to:

o Governance in the form of risk management strategy, expectations and policies

o Identification of risk to ships and ship/port interfaces

o Protection by implementation of risk control processes and measures, and contingency planning

o Detection by development, implementation and practice of activities necessary to detect a cyber incident event in a timely manner

o Response in form of activities and plans to minimize the effect of a detected cyber incident and provide resilience

CONARINA Head Office

6505 Blue Lagoon Dr. Suite 455
Miami, Fl., 33126
Tel: 1 (786) 558 5288,
Fax: 1 (786) 325 0200,
Joel@conarinagroup.com

o Recovery by implementing strategies for the recovery and reinstatement of essential business or mission critical assets or systems

• An updated list of Standards and Best Practices for Implementation of Cyber Risk Management, including reference to:

o IACS Unified Requirement E26 – Cyber resilience of ships, and

o IACS Unified Requirement E27 – Cyber resilience of onboard systems and equipment

---

REFERENCES:
- Maritime Cyber Risk Management (Msc-Fal.1/Circ.3/Rev.2)

ATTACHMENTS: No

Kindest Regards,
CONARINA Technical Office

CONARINA Head Office

6505 Blue Lagoon Dr. Suite 455
Miami, Fl., 33126
Tel: 1 (786) 558 5288,
Fax: 1 (786) 325 0200,
Joel@conarinagroup.com