INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3/Rev.3
4 April 2025

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard ships from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 The Maritime Safety Committee, at its 104th session (4 to 8 October 2021), and the Facilitation Committee, at its forty-sixth session (9 to 13 May 2022), approved an update to the additional guidance and standards included in paragraph 4.2 of the Guidelines.

4 The Maritime Safety Committee, at its 108th session (15 to 24 May 2024), and the Facilitation Committee, at its forty-ninth session (10 to 14 March 2025), approved a revision to the Guidelines on maritime cyber risk management, as set out in the annex.

5 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

6 This circular and any revisions supersede the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 INTRODUCTION

1.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, *maritime cyber risk* refers to a measure of the extent to which Computer Based Systems (CBS) are threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitalization, integration and automation of processes and systems in shipping.

1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and flag Administrations' requirements and guidance, as well as relevant international and industry standards and best practices.

1.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitalization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

1.5 Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization.

2 GENERAL

2.1 Key definitions

Computer Based System (CBS) means a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs on board include IT and OT systems. A CBS may be a combination of subsystems connected via a network. Onboard CBSs may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBSs and/or other facilities.

Cyber incident means an occurrence or a sequence of occurrences, which actually or potentially results in adverse consequences to a CBS or to the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and tolerating, terminating, transferring or treating it to an acceptable level by taking into consideration the costs and benefits of actions taken by stakeholders.

Information Technology (IT) refers to CBSs that are focused on the use of data as information, including software, hardware, and communication technologies (e.g. commercial information, or data about the crew, such as salaries, certificates, etc.).

Operational technology (OT) refers to CBSs that are focused on the use of data to control or monitor physical processes (e.g. the main engine's oil temperature levels, which are forwarded to the control room).

2.2 Background

2.2.1 Digital technologies, including CBS, have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and the Administration's requirements. However, the vulnerabilities created by accessing, interconnecting or networking with these systems can lead to cyberthreats and risks which should be addressed. Relevant systems could include, but are not limited to:

.1 Bridge systems, (such as navigation systems, ship safety systems, communications systems, etc.);

.2 Cargo, bunkering, lubrication, ballast and other pumping handling and management systems;

.3 Propulsion, fuel and machinery management and power control systems;

.4 Security, access control and surveillance systems;

.5 Passenger and crew servicing and management systems;

.6 Passenger, crew and subcontracted service personnel facing public networks;

.7 Administrative and crew welfare systems;

.8 Ship-port interfaces; and

.9 Ship-to-shore integrated systems (e.g. remote control systems/Maritime Autonomous Surface Ships).

2.2.2 When looking at CBSs, the distinction between information technology (IT) and operational technology (OT) systems should be considered. Furthermore, the protection of information during data exchange, storage and usage within these systems should also be considered. Vulnerabilities in the OT systems may increase the operational safety risks of ships that may jeopardize the safety of both crew and passengers. Therefore, OT systems should be segmented from IT systems, protected from Internet-facing systems and have appropriate protection tools.

2.2.3 While these technologies and systems provide significant efficiency gains for the maritime industry, they also present threats and risks to the operation of systems integral to shipping which, if affected, will have a safety, security and environmental impact. These risks may result from vulnerabilities arising from inadequate security-by-design, operation, integration, maintenance of systems or system patching, and from intentional and unintentional actions.

2.2.4 Cyber risks are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign careless actions (e.g. software maintenance or user permissions). In general, these actions can expose or exploit vulnerabilities (e.g. outdated software or ineffective firewalls) in CBSs. Effective cyber risk management should consider assessing and addressing both kinds of threats.

2.2.5 Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber hygiene. In general, where vulnerabilities in CBSs are exposed or exploited, either directly (e.g. weak passwords and/or careless password management leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for the confidentiality, integrity and availability of data, as well as implications for the safety and security of a ship, particularly where critical systems (e.g. bridge navigation, main propulsion systems, cargo on/off-loading systems) are compromised.

2.2.6 Effective cyber risk management should also consider risks posed by third-party vendors, embedded systems, and cyberthreats related to software and hardware supply chains of systems used in shipping. Account should also be taken of CBS maintenance devices and systems.

2.2.7 These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

2.2.8 In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should be taken into account, including amongst others, management, operational or procedural, and technical controls.

2.3 Application

2.3.1 These Guidelines are primarily intended for ships, and are designed to encourage safety and security management practices in the cyber domain.

2.3.2 Recognizing that no two ISM companies in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited digital systems may find a simple application of these Guidelines to be sufficient; however, ships with complex digital systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

3 ELEMENTS OF CYBER RISK MANAGEMENT

3.1 For the purpose of these Guidelines, *cyber risk management* means the process of identifying, analysing, assessing and communicating a cyber-related risk and tolerating, terminating, transferring or treating it to an acceptable level, considering costs and benefits of actions taken by stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyberthreats and risks. Safeguarding ships and ship-port interfacing systems from emerging threats should involve a range of controls that are continually evolving. Therefore, cyber resilient security features should be incorporated in the ship's equipment and systems at the design, manufacturing, integration, operation and maintenance stages.

3.3 Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal cybersecurity gaps in CBSs that can be addressed to achieve cyber resilience objectives through a risk-based approach. This risk-based approach is to evaluate the cyber risks, considering ship type and operational profile as well as onboard systems' complexity and connectivity, which will enable an organization to best apply its resources in the most cost-effective and efficient manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. The functional/technical cybersecurity controls listed under each of the functional elements represent the minimum controls that should be implemented. Additional cybersecurity controls may be considered depending on the evaluation of the identified cyber risks.

.1 Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.

.1 Designate a person or entity accountable for the planning, resourcing and execution of cybersecurity activities.

.2 Ensure that the designated person or entity is given the necessary authority and support to fulfil their duties and that they have sufficient knowledge and expertise in cyber risk management.

.2 Identify: Determine the current cyber risk to ships and ship/port interfaces.

.1 Identify the systems, assets, services, data and capabilities, interdependencies between safety critical systems (including the information flow) that, when disrupted, pose risks to ship operations, human safety, safety of the ship and/or a threat to the environment, including those related to the software and hardware supply chains.

.2 Establish and maintain an inventory of digital systems on board the ship. These systems and assets could include the systems listed in paragraph 2.2.1 of these guidelines. Identify internal and external systems dependencies and network connections.

.3 Carry out a risk assessment of those systems, services, assets, data and capabilities critical to ship operations, the sudden operational failure of which may result in hazardous situations. Identify cyber-related threats. Identify vulnerabilities to systems, services, assets, data and capabilities. Assess the likelihood and impact of a cyber incident on the safety, availability, integrity and confidentiality of those elements.

.3 Protect: Implement risk control processes and measures to protect CBSs, and contingency planning to protect against a cyber incident and ensure business continuity of shipping operations, human safety, safety of the vessel and/or threat to the environment.

.1 Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deactivate accounts for departing employees or users.

.2 Change all default passwords on all devices, enforce a strong password policy and consider establishing other user account access control management measures to safeguard against malicious attempts such as brute force attacks, phishing, etc. Use multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

.3 Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

.4 Implement security measures (such as firewall or antivirus) for any ship digital systems and devices that have access to the Internet or the company's intranet, or any interaction with third party or landside network and information systems, particularly those of ship/port interfaces. Implement policies and procedures regarding the use of cryptography.

.5 Establish controls to protect systems from the use of unauthorized removable media.

.6 Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises.

.7 Perform regular system backups, software updates, and develop and maintain incident response (IR) plans.

.8 Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.

.9 Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.

.4 Detect: Develop, implement and practise activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.

.1 Maintain a list of relevant threats, threat actor tactics, techniques and procedures and actively monitor systems for those threats.

.2 Annual basic cybersecurity training for all employees should include training on recognizing and detecting an ongoing cyber incident.

.5 Respond: Develop, implement and practise activities and plans to provide resilience and to restore systems necessary for shipping and ship-port operations or services impaired due to a cyber incident. Implement appropriate measures to minimize the effect of a detected cyber incident to other parts of ship systems.

.1 Report incidents to necessary parties within required time frames as defined by the Administration.

.2 Records of cyber incidents should be kept.

.3 Annual basic cybersecurity training for all employees should include training on responding to a cyber incident.

.6 Recover: Identify and implement measures to restore onboard CBS including networks necessary for shipping operations impacted by a cyber incident.

.1 Develop, maintain and implement strategies for the recovery and reinstatement of essential business or mission critical assets or systems that might be impacted by a cyber incident.

.2 Annual basic cybersecurity training for all employees should include training on recovering from a cyber incident.

.3 Carry out root cause analysis of cyber incidents, with the objective of resolving underlying issues and vulnerabilities to prevent similar recurrence.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms. Any documents, or sections of documents, developed to satisfy these functional elements should be protected by procedures aimed at preventing unauthorized access, deletion, destruction or amendment.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

3.8 Implementation of cyber resilient equipment and systems is to be considered. As part of technical measures, equipment and systems should be designed and tested as per international standards and guidance to assure cyber resilience on board ships.

4 STANDARDS AND BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to the Administration requirements, as well as relevant international and industry standards and best practices.*

4.2 Additional standards may include, but are not limited to:

.1 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.2 IACS UR E26 – International Association of Classification Societies Unified Requirement E26 – Cyber resilience of ships.

.3 IACS UR E27 – International Association of Classification Societies Unified Requirement E27 – Cyber resilience of onboard systems and equipment.

4.3 Additional guidelines and industry best practices may include, but are not limited to:

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.

.2 Consolidated IACS Recommendation on cyber resilience (Rec 166).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST 2.0 Framework).

.4 IAPH Cybersecurity Guidelines for Ports and Port Facilities.

4.4 Reference should be made to the most current version of any guidance or standards utilized.

4.5 Further references may be found on the IMO website under "Maritime cyber risk", and IMO Members are encouraged to forward references for relevant guidance and standards to the IMO Secretariat for inclusion on the IMO public website.

---

* The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.