Council of the
European Union

Brussels, 15 January 2024
(OR. en)

5460/24

MAR 8
OMI 10
CYBER 7

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 January 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2024) 14 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing the revision of the 2017 Guidelines on Maritime Cyber Risk Management

Delegations will find attached document SWD(2024) 14 final.

Encl.: SWD(2024) 14 final

EUROPEAN
COMMISSION

Brussels, 15.1.2024
SWD(2024) 14 final

COMMISSION STAFF WORKING DOCUMENT

Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing the revision of the 2017 Guidelines on Maritime Cyber Risk Management

Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing the revision of the 2017 Guidelines on Maritime Cyber Risk Management

PURPOSE

This Staff Working Document contains a draft Union submission to the International Maritime Organization's (IMO) 108th Maritime Safety Committee (MSC 108). The IMO has scheduled MSC 108 from 15 to 24 May 2024.

The draft submission is proposing the revision of the document MSC-FAL.1/Circ.3/Rev.2 on *the Guidelines on Maritime Cyber Risk Management*. The proposed revision of the Guidelines is intended to provide a harmonization of requirements within existing frameworks. The purpose is to set and ensure a level playing field and predictability on board ships regarding what to expect during surveys and inspections with respect to cyber risk management.

EU COMPETENCE

Regulation (EC) No 725/2004 on enhancing ship and port facility security[1] and Directive 2005/65/EC on enhancing port security[2] implement the maritime security regime agreed by the IMO in December 2002 in the International Convention for the Safety of Life at Sea (SOLAS) chapter XI/2 and the International Ship and Port Facility Security (ISPS) Code.

Regulation (EC) No 725/2004 also renders some provisions of Part B of the ISPS Code mandatory. Several sections under the ISPS Code are relevant to cybersecurity, notably the requirement to take computer systems and networks into account: Regulation (EC) No 725/2004, Annex III, paragraphs 8.3.5 and 15.3.5.

Cybersecurity was first horizontally regulated in the EU by Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union[3]. On 16 January 2023, Directive (EU) 2022/2555[4] (known as NIS2) entered into force replacing Directive (EU) 2016/1148. NIS2 Directive strengthens security requirements with a list of focused measures and streamlines incident reporting obligations. It significantly expands the scope of sectors and introduces a size threshold to define which entities fall in its scope, including in the water transport subsector. The EU Member States have until 17 October 2024 to transpose the Directive into their national legislative systems.

On 30 November 2023, a provisional political agreement was reached on the EU Cyber Resilience Act between the co-legislators, the European Parliament and the Council. The Cyber Resilience Act (CRA) mandates that products with digital elements, will only be made available on the market if they meet specific essential cybersecurity requirements. According to the provisional political agreement, the CRA shall not apply to marine equipment that falls within the scope of Directive 2014/90/EU. The CRA's cybersecurity requirements for hardware and software, including components, will significantly contribute to ensuring security of supply chain, including for the maritime sector. The CRA will help organisations defined as essential and important entities under the NIS2 Directive, such as critical infrastructure providers, including in the water transport subsector, meet their supply chain security obligations by providing them with assurance that the products they deploy exhibit a high level of cybersecurity and that their manufacturers will take the provision of security updates throughout their deployment time seriously. Once formally adopted, the CRA will enter into force on the 20th day following its publication in the Official Journal. The transition period agreed by the co-legislators for the CRA cybersecurity essential requirements is of 36 months. The CRA will also be followed by European harmonised standards to be developed by European Standardisation Organisations.

[1] OJ L 129, 29.4.2004, p. 6
[2] OJ L 310, 25.11.2005, p. 28
[3] OJ L 194, 19.7.2016, p. 1
[4] OJ L 333, 27.12.2022, p. 80

In light of all of the above, the present draft Union submission falls under EU exclusive competence, pursuant to article 3(2) TFEU.[5] This Staff Working Document is presented to establish an EU position on the matter and to transmit the document to the IMO prior to the required deadline of 13 February 2024.

[5] An EU position under Article 218(9) TFEU is to be established in due time should the IMO Maritime Safety Committee eventually be called upon to adopt an act having legal effects as regards the subject matter of the said draft Union submission. The concept of '*acts having legal effects*' includes acts that have legal effects by virtue of the rules of international law governing the body in question. It also includes instruments that do not have a binding effect under international law, but that are '*capable of decisively influencing the content of the legislation adopted by the EU legislature*' (Case C-399/12 Germany v Council (OIV), ECLI:EU:C:2014:2258, paragraphs 61-64). The present submission, however, does not produce legal effects and thus the procedure for Article 218(9) TFEU is not applied.

MARITIME SAFETY COMMITTEE
108th session
Agenda item 6

MSC 108/6/x
13 February 2024
Original: ENGLISH

Pre-session public release: ☒

REVISION OF THE *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT* (MSC-FAL.1/CIRC.3/REV.2) AND IDENTIFICATION OF NEXT STEPS TO ENHANCE MARITIME CYBERSECURITY

Proposed revision of the 2017 Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2)

Submitted by Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands (Kingdom of the), Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the European Commission[6], acting jointly in the interest of the European Union

SUMMARY

Executive summary:	This document proposes a revision of document MSC-FAL.1/Circ.3/Rev.2 on *Guidelines on Maritime Cyber Risk Management*. The proposed revision of the Guidelines is intended to provide a harmonization of requirements within existing frameworks. The purpose is to set and ensure a level playing field and predictability on board ships regarding what to expect during surveys and inspections with respect to cyber risk management.
Strategic direction, if applicable:	1, 2, 5 and 6
Output:	
Action to be taken:	23
Related documents:	MSC-MEPC.1/Circ.5/Rev.4; MSC-FAL.1/Circ.3/Rev.2; resolution A.1110(30); resolution MSC.428(98); MSC.1/Circ.1526; MSC-MEPC.7/Circ.1; MSC 107/17/9 and MSC 107/20

Introduction

1 This document is submitted in accordance with paragraphs 4.6 and 6.12.2 of the *Organization and method of work of the Maritime Safety Committee and the Marine Environment Protection Committee and their subsidiary bodies* (MSC-MEPC.1/Circ.5/Rev.4) and proposes to review and update MSC-FAL/Circ.3/Rev.2 on *Guidelines on Maritime Cyber Risk Management*.

Background

[6] Australia, Singapore, United Kingdom and United States of America have stated their interest in being co-sponsors.

2 At its 107th session, the Maritime Safety Committee agreed to include in its biennial agenda for the 2024-2025 biennium and the provisional agenda of MSC 108 an output on "Revision of the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity", with a target completion year of 2024, inviting the FAL Committee to become an associated organ. This document is the proposed draft revision of MSC-FAL/Circ.3/Rev.2 on *Guidelines on Maritime Cyber Risk Management.*

3 As already highlighted by document MSC 107/17/9 (Australia et al.), the maritime industry is undergoing a significant transformation based on the increased use of cyber-connected systems. While these systems improve commercial vessel and port facility operations, they also entail increased cyber threats and risks. The number of cyber threats and incidents have risen in recent years and have the proven potential of seriously impeding international maritime transport operations.

4 Document MSC-FAL.1/Circ.3/Rev.2 on *Guidelines on Maritime Cyber Risk Management* (Guidelines) and resolution MSC.428(98) on *Maritime Cyber Risk Management in Safety Management Systems* provide useful indications on how vessels should address cyber risk. However, since the cyber threats have evolved, a proposed revised guidelines on the cyber risk management measures and procedures being put in place would aid Administrations, shipowners and ship operators, as well as port States and port facilities, to increase the level of their maritime safety and security awareness, while retaining a level of flexibility to enable different maritime industry players to adapt the appropriate measures for their own practices and activities.

Analysis of the issue

5 IMO is the recognized entity for issues pertaining to international shipping and is the appropriate forum to set global standards to address cybersecurity throughout the global marine transportation system.

6 Enhanced Guidelines will help establish a more easily understandable baseline level of protection from cyber threats throughout the international maritime network of ships. Several aspects of the Guidelines may benefit from an update.

7 A revision of the Guidelines should also take into account, to the extent possible, recent relevant horizontal cybersecurity frameworks and standards with global implications, such as legislative frameworks setting out cybersecurity requirements for hardware or software or technical, operational and organisational cybersecurity risk management and incident reporting requirements that strengthen the security of supply chain.

8 A revision of the Guidelines should consider what measures may best protect against cyber incidents that may compromise the functioning of operations of maritime assets. Both information (IT) and operational (OT) technologies are relevant in this regard. A higher reliance on IT and OT systems by an entity or asset should entail stronger cyber risk management measures.

9 Identifying assets that are vulnerable to cyber threats and risks is an essential step in being able to protect an entity. The Guidelines already provide a list of potentially vulnerable systems in shipping, but it should be considered whether this list needs to be updated.

10 Personnel have a key role in mitigating cyber risks. Raising awareness of basic cyber hygiene is a simple measure which can result in more cyber resilience. Annual basic cybersecurity training can raise awareness and ensure that personnel adopt the right reflexes and behaviours. There should be an emphasis on the training of OT users. Where

cyber resilience and response plans are developed, aspects of these can be integrated into training, to familiarise personnel with the roles and actions to carry out. Assigning roles and responsibilities within an entity, as well as acquiring or building the right expertise, are other measures that can be vital in mitigating cyber risks.

11 More detailed measures may be especially useful when describing protective means and processes to put in place against cyber threats and to ensure the business continuity of shipping operations. Several elements should be taken into account in order to update the Guidelines. Software and hardware supply chains security is, for example, an aspect of cyber risk management which has gained more attention in recent years. Particular attention should be given to ensuring that deployed software and hardware has been developed in line with state-of-the-art security-by-design principles and that their manufacturers have put in place vulnerability handling processes that ensure that vulnerabilities are addressed throughout the lifetime of a product. It is also suggested that important measures such as user account access control and the timely updating of software are included in the Guidelines. Special attention should also be brought to ship-port interfacing systems.

12 The Guidelines should encourage the reporting of cyber incidents. Reporting of incidents is an important element in allowing Contracting Governments not only to respond, but also to be aware of the threat posed, and if necessary to develop more robust procedures or adopt a heightened security posture. This entails that procedures are in place and roles are assigned for the reporting of incidents to Contracting Governments.

Analysis of the implications

13 The proposed revision of the Guidelines is intended to provide a harmonization of requirements within existing frameworks. The purpose is to set and ensure a level playing field and predictability on board ships regarding what to expect during surveys and inspections with respect to cyber risk management.

14 The proposed revision of the Guidelines would encourage more robust cyber risk management measures which, if applied in full, may induce administrative and implementation costs on the maritime industry. However, as the Guidelines remain non-mandatory, there remains flexibility in how Contracting Governments and the maritime industry apply them. The proposed revision of the Guidelines aims to remain non-prescriptive and allow flexibility in its implementation. In addition, the intention of the revision is to ease administrative burdens by simplifying procedures and harmonizing demands. More robust cyber management measures are also likely to save costs in the long term while allowing the maritime industry to fully enjoy the advantages of digitalisation, by reducing the occurrence of cyber incidents.

Benefits

15 The co-sponsors are of the view that the benefit of the revision of the Guidelines will provide a more uniform approach to demands on cyber risk management, further promote a culture of cybersecurity in the maritime domain, and will support predictability and a level playing field for seafarers and the industry. It will improve safe and secure shipping by enhancing cyber resilience and protecting global supply chains.

16 Both the maritime industry and Administrations could benefit from more detailed, universal guidelines related to cyber risk management. Updated guidelines could improve the baseline level of protection from cyber risk throughout the global marine transportation system.

17 A review of the Guidelines and identification of next steps will align with strategic directions 1, 2, 5 and 6 by applying consistency in the application of the Guidelines by Member States, protecting the maritime industry while it integrates new technologies, raise global security levels, and enable better regulation of cyber readiness throughout the global marine transportation system.

Human element

18 The proposed revision of the Guidelines intends to provide simple, clear and comprehensive non-mandatory guidance instructions to ship owners, operators and seafarers to assist them in addressing cyber risk management. Their full implementation may require the cooperation of crew members, for example in the raising of awareness on cyber hygiene or through participation in training, and may require additional cyber risk management measures to be taken, but should not constitute an undue burden to all staff including ship crew members and shore based personnel. The proposal is considered to have positive implications for the human element as it will help ensure predictability for seafarers regarding procedures on board ship.

Industry standards

19 The Guidelines include reference to existing industry standards and best practices on maritime cyber risk management:

.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 *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).

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

.5 IAPH Cybersecurity Guidelines for Ports and Port Facilities.

20 It is proposed that this list of existing industry standards and best practices be maintained in the revision of the Guidelines, as these are well established publications on cyber risk management within the maritime community. However, additional cybersecurity requirements, standards, and guidance has been published since the release of the Guidelines. These include, in particular, IACS unified requirements E26 *Cyber resilience of ships*, E27 *Cyber resilience of on-board systems and equipment*, and the updated language in the NIST Framework (NIST 2.0). As these are well established publications within the maritime community, it is proposed to add these to the existing list, and differentiate between standards, and guidelines and industry best practices.

21 In order to raise awareness on other new requirements, standards, and guidance materials, it is proposed that IMO members and observers be invited to submit publications that they believe are relevant to the IMO Secretariat, for inclusion in a list to be published on the IMO's website. This would provide a more flexible way to regularly update the list of relevant publications, as the amount of useful literature on maritime cyber risk management steadily increases. An example is the Guidelines for cybersecurity in the maritime sector of the European Union Agency for Cybersecurity (ENISA) from December 2020.

Proposal

22 It is proposed that the Committee revise the *MSC-FAL/Circ.3/Rev.2 on Guidelines on Maritime Cyber Risk Management* as detailed in Annex 1.

23 It is proposed that members and observers be invited to submit publications relevant to maritime cyber risk management to the IMO Secretariat for inclusion in the list of "Other guidance and standards" available on the IMO's webpage on Maritime cyber risk: Maritime cyber risk (imo.org)

Actions requested of the Committee

24 The Committee is invited to consider the proposed revision of the Guidelines referred to in paragraph 22 and the proposal concerning publications on maritime cyber risk in paragraph 23.

ANNEX 1

PROPOSED REVISION OF THE *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*

(Proposed changes are shown in additions/~~deletions~~)

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
~~30 November 2023~~
X XXX 2024

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*~~, as set out in the annex~~.

2 The Guidelines provide high level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats 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 (X to X May 2024), and the Facilitation Committee, at its X session (X to X XXX 2024), 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 ~~a technology asset is~~ 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 ~~digitization~~ 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 ~~digitization~~ 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 onboard include IT and OT systems. A CBS may be a combination of subsystems connected via 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, which actually or potentially results in adverse consequences to an onboard system, network and computer 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) means systems focusing on the use of data as information, including software, hardware, and communication technologies (i.e., data about the crew, such as salaries, certificates etc.).

Operational technology (OT) means systems focusing on the use of data to control or monitor physical processes (i.e., the main engine's oil temperature levels, which are forwarded to the control room).

2.2 Background

2.2.1 ~~Cybertechnologies~~ Digital technologies 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 Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking with these systems can lead to cyber threats and risks which should be addressed. ~~Vulnerable systems~~ Relevant systems could include, but are not limited to:

.1 Bridge systems, (e.g. navigation systems, ship safety systems, communications systems, etc.);
.2 Cargo, bunker and ballast handling and management systems;
.3 Propulsion, fuel and machinery management and power control systems;
.4 Security, ~~A~~access control and surveillance equipment systems;
.5 Passenger servicing and management systems;
.6 Passenger and crew facing public networks;
.7 Administrative and crew welfare systems; ~~and~~
.8 Ship-port interfaces; and
.9 ~~Communication systems~~ Ship to shore integrated systems (e.g. remote control systems).

2.2.2 When looking at CBS the distinction between information technology (IT) and operational technology (OT) systems should be considered. ~~Information technology~~ IT systems may be ~~thought of~~ considered as focusing on the use of data as information including software, hardware, and communication technologies (i.e., data about the crew, such as salaries, certificates etc.). ~~Operational technology~~ OT systems may be ~~thought of~~ considered as focusing on the use of data to control or monitor physical processes (i.e., the main engine's oil temperature levels, which are forwarded to the control room). Furthermore, the protection of information ~~and~~ during data exchange, storage and usage within these systems should also be considered. Vulnerabilities in the OT systems may increase risk to the operational safety of ships and cause a physical impact. Therefore, OT systems should be protected from Internet-facing systems and IT systems with segregation and appropriate protection tools, such as uni-directional data diode.

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 safety, security and environmental impact ~~risks to critical systems and processes linked to the operation of systems integral to shipping~~. These risks may result from vulnerabilities arising from inadequate security-by-design, operation, integration, maintenance ~~and design~~ of ~~cyber-related~~ systems, and from intentional and unintentional actions ~~cyberthreats~~.

2.2.4 ~~Threats~~ 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 CBS ~~or exploit a vulnerability in operational or information technology~~. 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 ~~discipline~~. In general, where vulnerabilities in ~~operational and/or information technology~~ CBS are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for ~~security and~~ the confidentiality, integrity and availability of data, as well as ~~information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be~~ implications for the safety and security of a ship, particularly where critical systems (e.g. bridge navigation~~, or~~ main propulsion systems, cargo on/off-loading systems) are compromised.

2.2.6 Effective cyber risk management should also consider risk posed by third-party vendor and cyber threats related to software and hardware supply chains of systems used in shipping. ~~safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).~~

~~2.1.7 Further information regarding vulnerabilities and threats can be found in the additional guidance and standards referenced in section 4.~~

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 ~~also~~ be taken into ~~consideration~~ account, including amongst others, management, operational or procedural, and technical controls.

2.3 Application

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

2.3.2 Recognizing that no two organizations 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 ~~cyber-related~~ systems may find a simple application of these Guidelines to be sufficient; however, ships with complex digital ~~cyber-related~~ systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.3.3 These Guidelines are recommendatory.

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 ~~accepting,~~

~~avoiding, transferring, or mitigating~~ tolerating, terminating, transferring or treating it to an acceptable level, considering costs and benefits of actions taken ~~to~~ by stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber threats and risks. Safeguarding vessels and ship-port interfacing systems from emerging threats must involve a range of controls that are continually evolving. Therefore, it is necessary to incorporate cyber resilient security features 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 CBS that can be addressed to achieve ~~risk management~~ cyber resilience objectives through a risk-based approach ~~prioritized cyber risk management plan~~. This risk-based approach 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:

.1 Govern: Establish and monitor risk management strategy, expectations, and policies. Define personnel roles and responsibilities for cyber risk management.

.1 Designate a person accountable for the planning, resourcing, and execution of cybersecurity activities. Ensure business continuity, such as backup management and disaster recovery, and crisis management.

.2 Ensure that the designated person 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: ~~Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.~~ Determine the current cyber risk to ships and ship/port interfaces.

.1 Identify the systems, assets, services, data and capabilities that, when disrupted, pose risks to ship operations, including those related to the software and hardware supply chains.

.2 Establish and maintain an inventory of digital systems onboard 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 that have been identified as important to ship operations.

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 CBS, and contingency planning to protect against a cyber incident ~~event~~ and ensure business continuity of shipping operations.

.1 Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deprovision 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 Company's intranet, or any interaction with third party or landside network and information systems, particularly those of port facilities. Implement policies and procedures regarding the use of cryptography and, where appropriate, encryption.

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

.6 Mandate annual basic cybersecurity training for all employees and OT specific cybersecurity training for OT users. 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 important.

.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, ~~and~~ implement and practice activities necessary to detect a cyber incident ~~event~~ in a timely manner.

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

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

.5 Respond: Develop, ~~and~~ implement and practice 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 ~~event~~.

.1 Report incidents to necessary parties within required timeframes as defined by 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 measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident ~~event~~.

.1 Develop, maintain, and execute plans to recover and restore to service 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 to resolve 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 unauthorised 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.

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 Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional ~~guidance and~~ standards may include, but are not limited to[7]:

.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 on-board systems and equipment.

4.3 Additional guidelines and industry best practices 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.

[7] 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.