Proposals for Effective Cyber Risk Management

Presented by Mersea

Contents

Why is cyber security important?

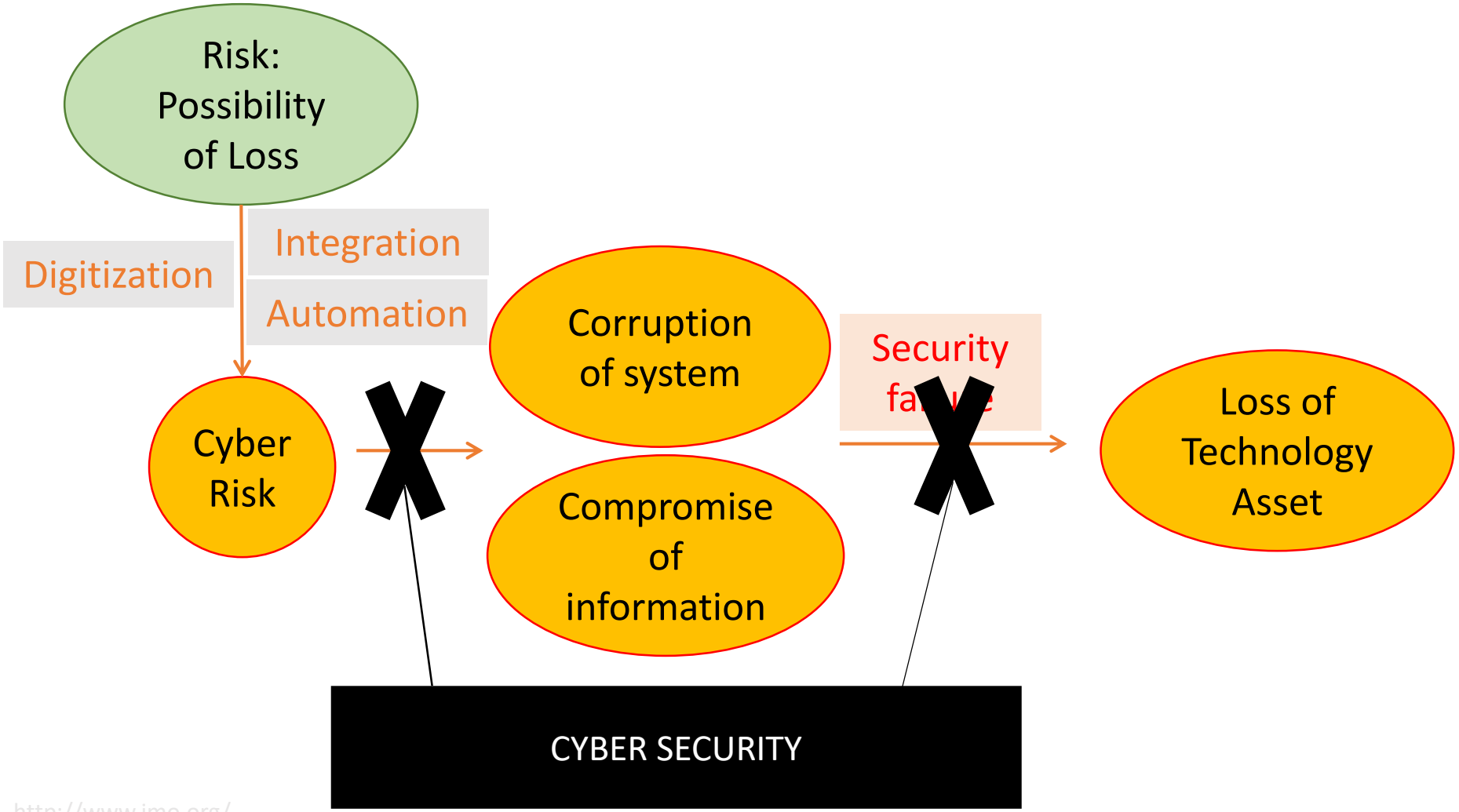
IMO and Cybersecurity

Proposals for Effective Cyber risk management

01. Issues at Hand

01. Issues at Hand

What is Cyber security?



http://www.imo.org/

01. Issue at Hand

Cyber Security as IMO Strategy Direction

SD 5: Enhance global facilitation and security of international trade

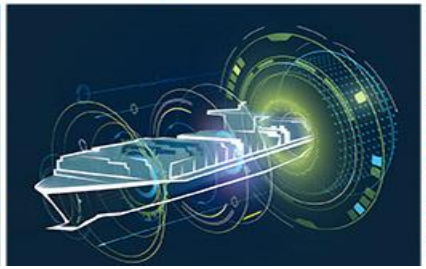
Outcome 5.2 Guidelines and guidance on the implementation and interpretation of SOLAS chapter XI-2 and the ISPS Code

SD 6: Ensure regulatory effectiveness

Outcome 6.1 Unified interpretation of provisions of IMO safety, security, and environment-related conventions






01. Issue at Hand

IMO and Cybersecurity

2014 July

With Canada mentioning 'cyber security' in FAL 39/7 for the first time, IMO recognized CS as a crucial issue.

2014 Nov

Delegate states have recognized the need to raise awareness of cybersecurity

(MSC 94~ 101)

2017 June

MSC 428 (98) was passed stating that CRM must be included in DOC before January 2021.

2019 March

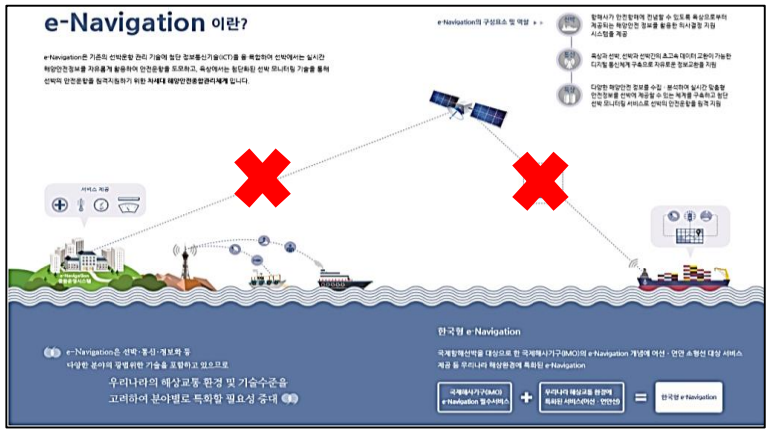
The Industry Guidelines on cyber security on board ships, version 3

(MSC 101/4/1)

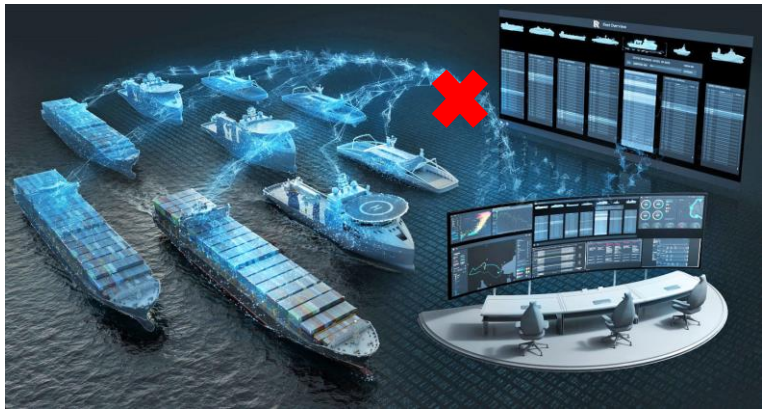
Two important Documents
MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management
MSC.428(98) Maritime cyber risk management in safety management systems

01. Issue at Hand

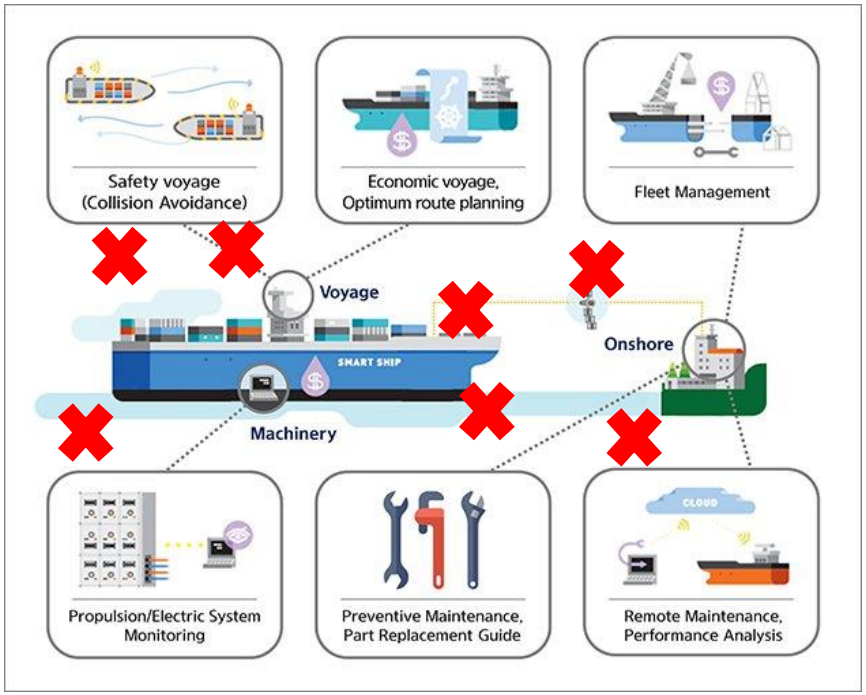
Increasing Importance of Cyber Security: Tech development



E-Navigation System



Autonomous Vessel (Rolls Royce)



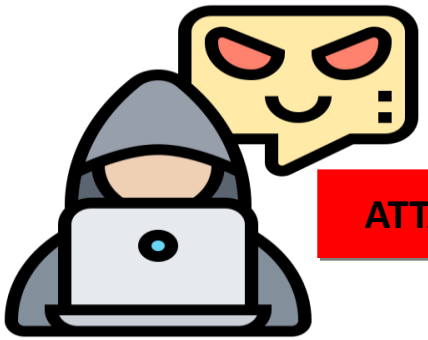
Integrated Smart Ship Solution(HHI)

Increase in **Connectivity**
-> Increase in **Efficiency**
-> Increase in **Cyber Risk**

Korean Register, Roll Royce, Hyundai Heavy Industries

01. Issue at Hand

SHOCK: 2017 Maersk Incident



NotPetya
(ransomware)

ATTACK

SHUT DOWN

130 Countries

$300M

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

01. Issue at Hand

After Maersk incident: **Insufficiency of cyber security**

1. Cyber security is still breached

July 2018

COSCO at the Long Beach Port terminal

September 20, 2018

Several servers in the Port of Barcelona's security infrastructure.

September 2018

San Diego port

May 2019

USCG warned of cyber attacks.

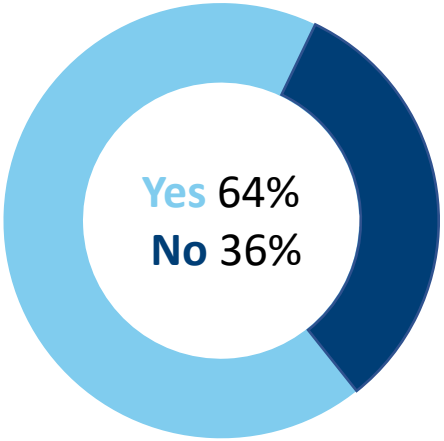
Who's next?

01. Issue at Hand

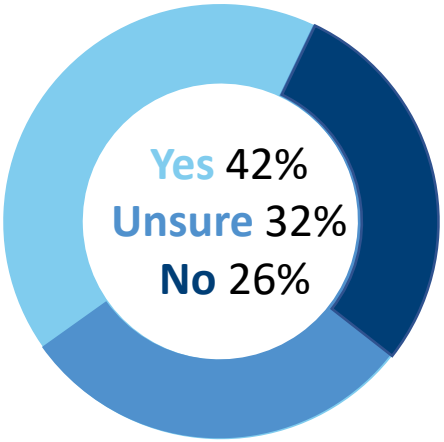
After Maersk incident: **Insufficiency of cyber security**

2. Cyber security is still insufficient

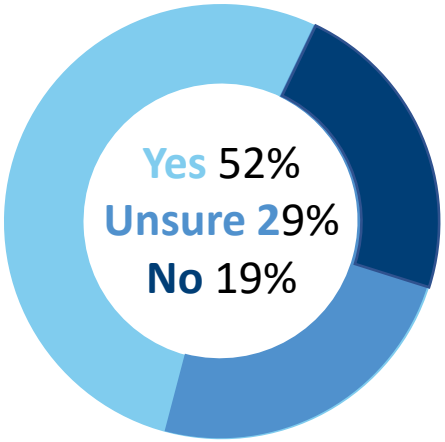
Do you provide cyber-risk awareness training to staff?



Does your company protect your vessels from OT cyber threats?



Does your organization have a business continuity plan in the event of a cyber incident?



A third of the respondents are still not sure about their cyber risk management system.

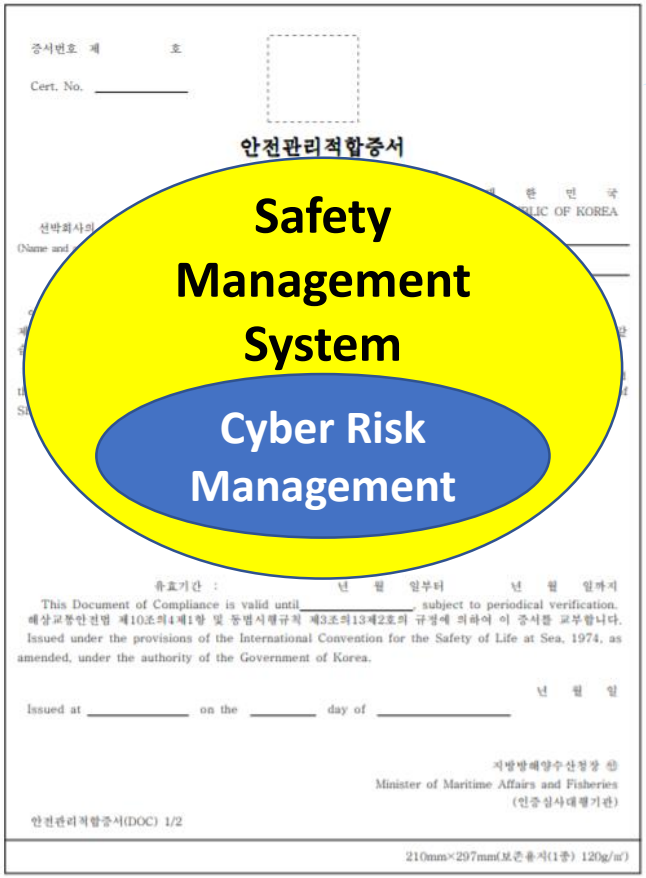
Safety at Sea and BIMCO cyber security whitepaper 2019

02. Analysis

02. Analysis

Analysis on Current Status

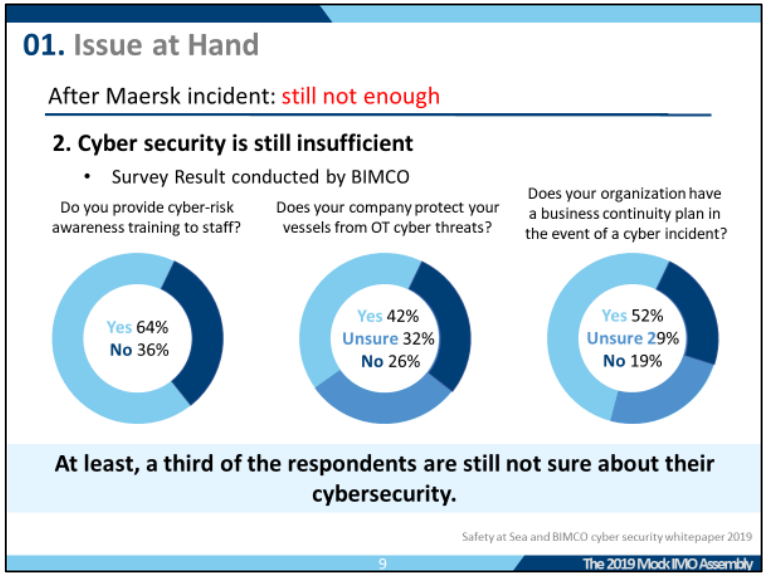
Issue DOC
Until Jan.01.2021



Are Shipping Companies ready?

NOT YET!

Shipping Companies



02. Analysis

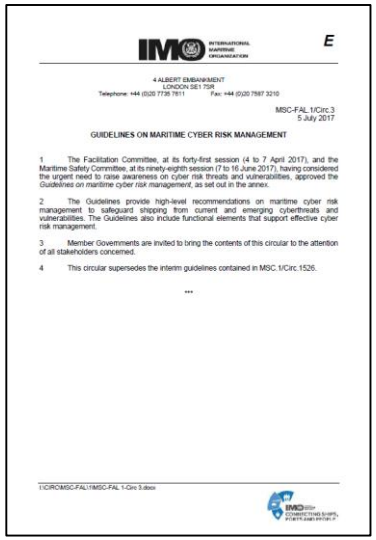
Analysis on Current Status

Shipping Companies are not ready to manage Cyber Risk effectively, because of…

① **Vagueness in the IMO Documents about the implementation of Cyber Risk Management(CRM)**

② **Legal status of the guidelines : non-mandatory**

Vagueness about the implementation of CRM



E

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

MSC-FAL.1/Circ.3
5 July 2017

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.

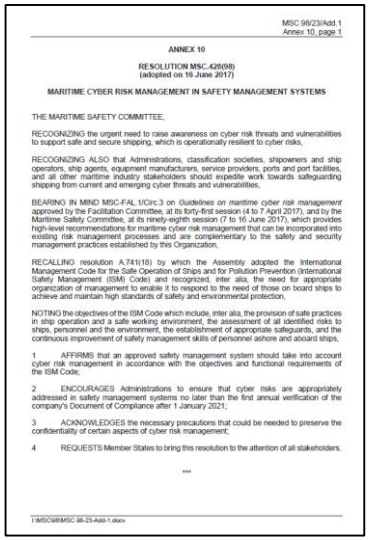
2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

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

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

I:\CIRC\MSC-FAL\1\MSC-FAL.1-Circ.3.docx



MSC 98/23/Add.1
Annex 10, page 1

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

I:\MSC\98\MSC 98-23-Add-1.docx

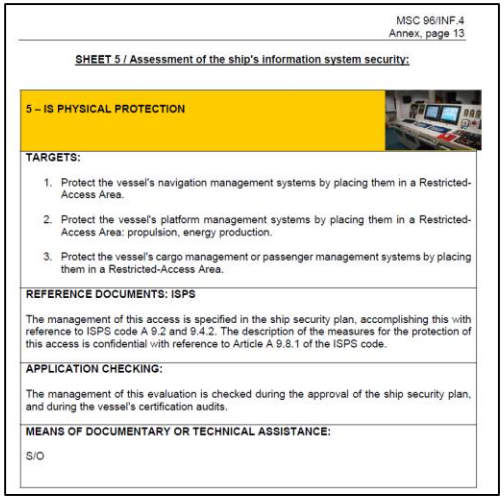
Guidelines MSC-FAL.1/Circ.3 Resolution MSC.428(98)

The Guidelines and the Resolution offer only the definition of effective Cyber Risk Management through five functional requirements, but **not the specific methods to implement and carry out Cyber Risk Management.**

02. Analysis

Vagueness about the implementation of CRM

MSC 96th session, there was a discussion about methodology



MSC 96/INF.4
Annex, page 13

SHEET 5 / Assessment of the ship's information system security:

5 – IS PHYSICAL PROTECTION

TARGETS:

1. Protect the vessel's navigation management systems by placing them in a Restricted-Access Area.
2. Protect the vessel's platform management systems by placing them in a Restricted-Access Area: propulsion, energy production.
3. Protect the vessel's cargo management or passenger management systems by placing them in a Restricted-Access Area.

REFERENCE DOCUMENTS: ISPS

The management of this access is specified in the ship security plan, accomplishing this with reference to ISPS code A 9.2 and 9.4.2. The description of the measures for the protection of this access is confidential with reference to Article A 9.8.1 of the ISPS code.

APPLICATION CHECKING:

The management of this evaluation is checked during the approval of the ship security plan, and during the vessel's certification audits.

MEANS OF DOCUMENTARY OR TECHNICAL ASSISTANCE:

S/O

MSC/96/INF.4(France)

…The development of international cyber risk management guidelines for ships will provide an assessment and management tool to assist owners, operators and administrations in educating, communicating, deterring and responding to cyber risks that threaten the safe operation of ships.

MSC 96/4/2, paragraph 7 (Canada, Japan, Norway, US, etc.)

However, delegates and the Legal Affairs and External Relations Division expressed doubt on self-assessment tools for Cyber Risk Management because of **the lack of accumulation of best practices and experience.**

Vagueness about the implementation of CRM

Improved capability to develop guidance

BIMCO's Guidelines on Cybersecurity version 3

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

Update	Description of Update
Clarified that terms like "compliance" can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing.
A new section on self-assessment	Added Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.

NIST Cybersecurity Framework version 1.1

Need and Capability to make clear guidance to implement Cyber Risk Management System

02. Analysis

Legal status of the guidelines as non-mandatory

- Guidelines MSC-FAL.1/Circ.3

2.2.3 These Guidelines are recommendatory.

- Resolution MSC.428(98)

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

02. Analysis

Legal status of the guidelines as non-mandatory

Ongoing discussion,

MSC 97/4, Islamic Republic of Iran

Hence, it seems that **developing a mandatory and verifiable code** should be taken into consideration by all Member States, at least for near future

MSC 98/23 paragraph 5.5

5.5 …**some delegations were of the view that the mandatory implementation of maritime cyber risk management was an issue**, agreed that **this would require further consideration after gaining more experience from the use of the guidelines**.

MSC 98/23 paragraph 5.7.5

the adoption of an MSC resolution to introduce the use of non-mandatory guidelines as part of safety management systems could be contrary to the principle of the ISM Code and an **alternative solution could be amending MSC.1/Circ.1371**

02. Analysis

Legal status of the guidelines as non-mandatory

Improved capability to develop a guidance

BIMCO's Guidelines on Cybersecurity version 3

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

Update	Description of Update
Clarified that terms like "compliance" can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing.
A new section on self-assessment	Added Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.

NIST Cybersecurity Framework version 1.1

MSC 101/24 paragraph 4.9

a number of delegations **expressed the need for clarification that effective cyber risk management had to be included in SMS**,

With the accumulation of experience and the updated industry guidelines over the last few years, **it is time to enforce** the mandatory implementation of CRM.

Summary of Analysis

Two problems in implementing effective cyber risk management

① **Vagueness in the IMO Documents about the implementation of Cyber Risk Management(CRM)**

② **Legal status of the guidelines as non-mandatory**

02. Analysis

Summary of Analysis

Two problems in implementing effective cyber risk management

① **Vagueness in the IMO Documents about the implementation of Cyber Risk Management(CRM)**

=> **Propose to include Cyber risk self assessment in the Guidelines**

② **Legal status of the guidelines as non-mandatory**

=> **Propose to amend ISM code and MSC.1/Circ.1371**

03. PROPOSALS

03. Proposals

Proposals for effective cyber risk management

① Revise the Guidelines(MSC-FAL.1/Circ.3) to include cyber risk self assessment procedure

② Include the Guidelines in MSC.1/Circ.1371.

③ Amend Safety management objectives in paragraph 1.2.2.1 of ISM Code

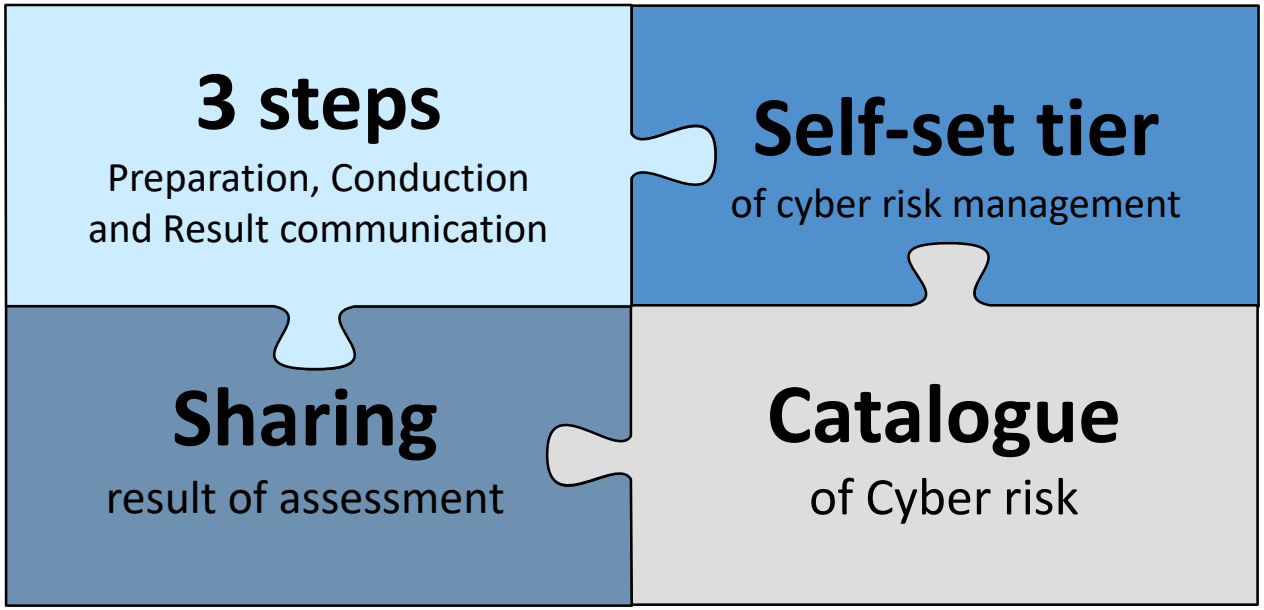
03. Proposals

① Include Cyber risk self assessment: Concept

- **Goal of cyber risk self assessment**

: to encourage organizations to identify and mitigate risks and vulnerabilities of cyber threats.

- 4 essential elements in cyber risk assessment



03. Proposals

① Include Cyber risk self assessment: Revision

REVISION OF THE GUIDELINES ON MARITIME CYBER RISK MANAGEMENT(MSC-FAL.1/CIRC.3)

3 ELEMENTS OF CYBER RISK MANAGEMENT

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an ~~organization~~'entity's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. The method of self assessment is the best application of this approach. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

When applied to cyber risk self assessment, effective self assessment requires four elements:

.1 The Self-assessment procedure must consist of at least these 3 steps:
Preparation, Conduct and Result communication and feedback

.2 each entity should select from self-set tier of cyber risk management

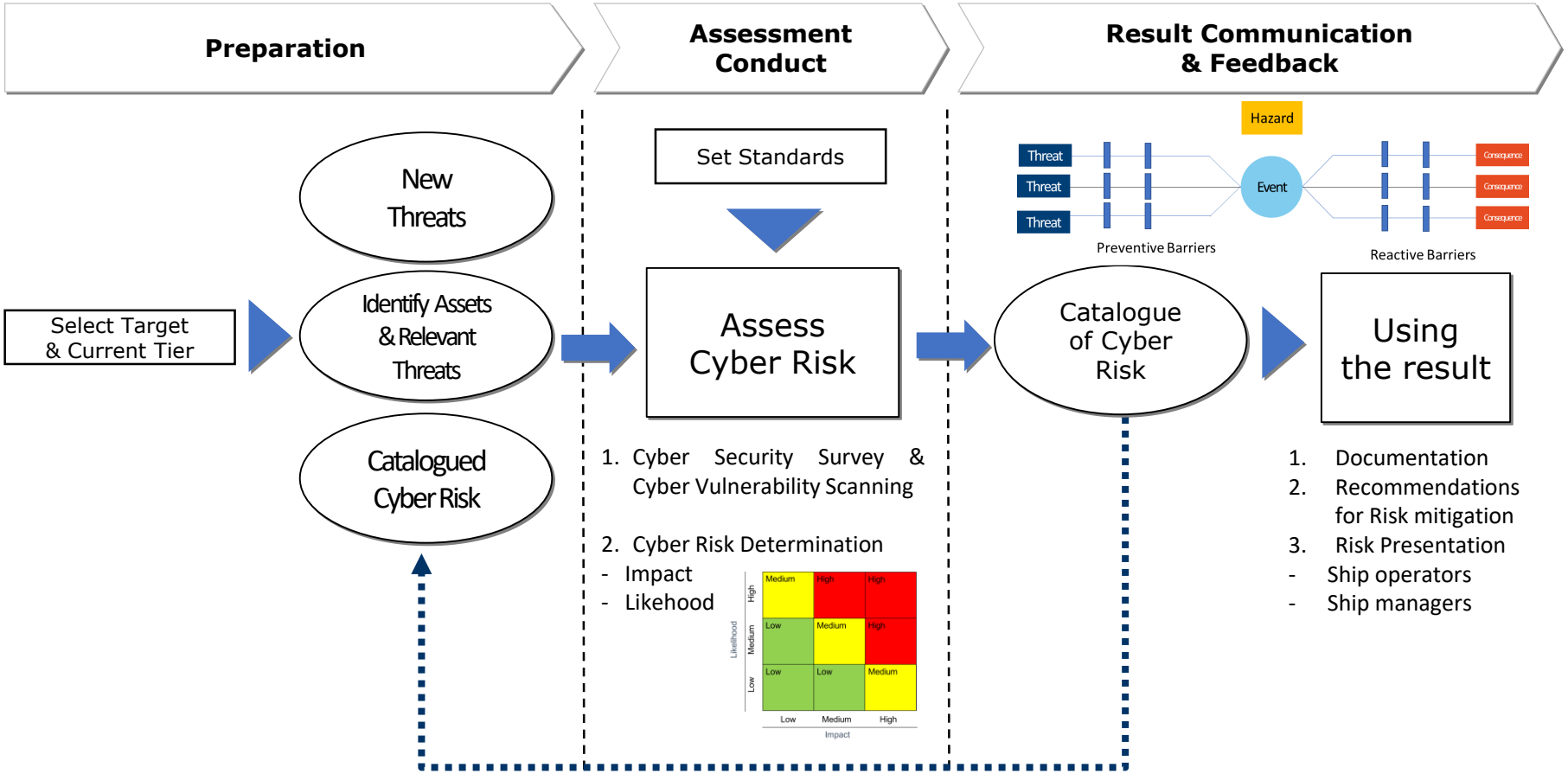
.3 make Catalogue of Cyber risk should be developed and stored in the entity

.4 result of assessment should be shared with field operators and managers

To help implementation of cyber risk self assessment, Annex 3 is recommended.

03. Proposals

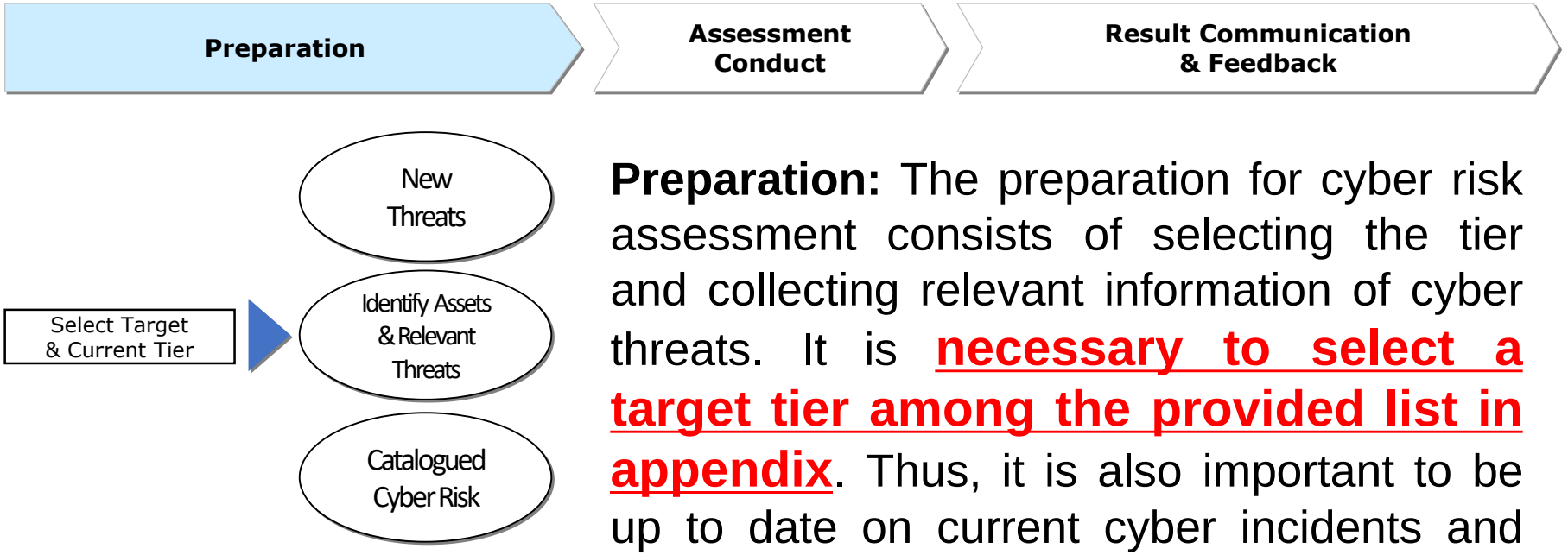
① Include Cyber risk self assessment: Appendix



** This cyber risk self assessment procedure is referred from the guidelines on maritime cybersecurity by KR, DNV-GL, Maritime Cyber Risk Management: An Experimental Ship Assessment(Boris Svilicic), and Cyber Threat Metrics(Mark Mateski)*

03. Proposals

① Include Cyber risk self assessment: Appendix



Preparation: The preparation for cyber risk assessment consists of selecting the tier and collecting relevant information of cyber threats. It is **necessary to select a target tier among the provided list in appendix**. Thus, it is also important to be up to date on current cyber incidents and issues. The entity should utilize results and reports from previous assessments.

** This cyber risk self assessment procedure is referred from the guidelines on maritime cybersecurity by KR, DNV-GL, Maritime Cyber Risk Management: An Experimental Ship Assessment(Boris Svilicic), and Cyber Threat Metrics(Mark Mateski)*

① Include Cyber risk self assessment: Appendix

Preparation | **Assessment Conduct** | **Result Communication & Feedback**

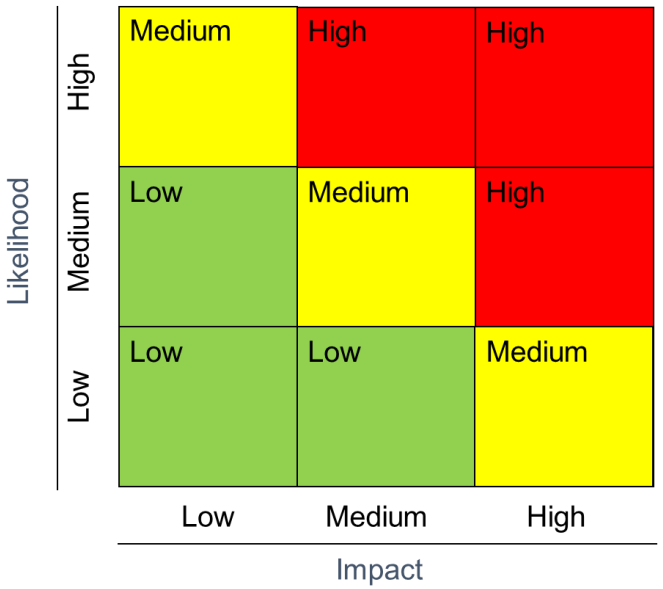
Conduct: The entity should **survey cyber security** and **scan vulnerability strictly under its discretion, referring to the Industrial Guidance**.

Set Standards

Assess Cyber Risk

1. Cyber Security Survey & Cyber Vulnerability Scanning

2. Cyber Risk Determination
- Impact
- Likehood



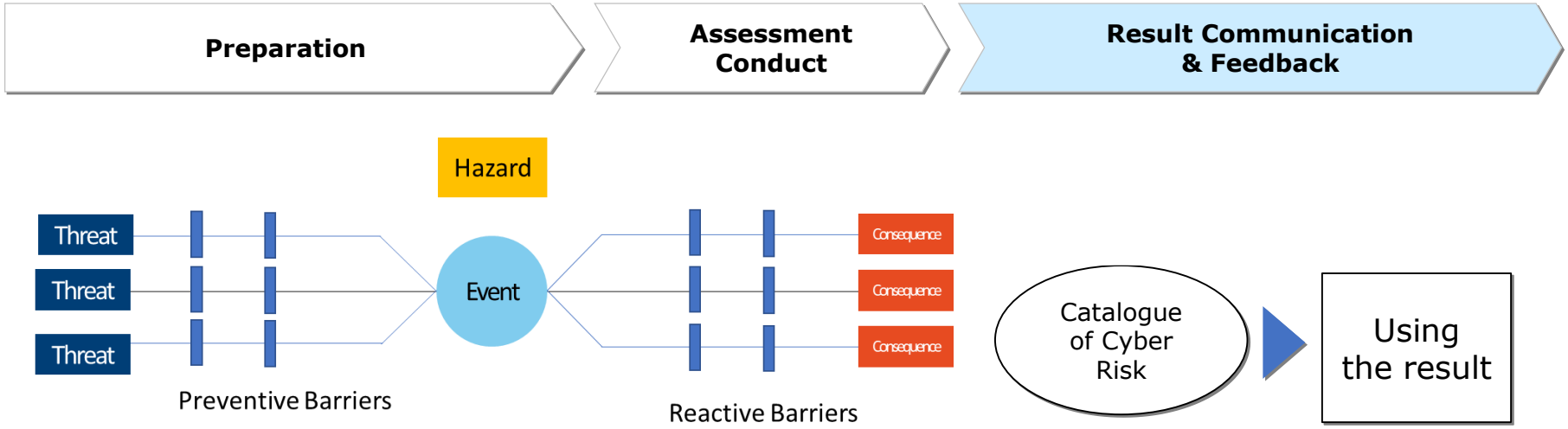
Cyber Risk Matrix

Information | Action

** This cyber risk self assessment procedure is referred from the guidelines on maritime cybersecurity by KR, DNV-GL, Maritime Cyber Risk Management: An Experimental Ship Assessment(Boris Svilicic), and Cyber Threat Metrics(Mark Mateski)*

03. Proposals

① Include Cyber risk self assessment: Appendix



1. Documentation
2. Recommendations for Risk mitigation
3. Risk Presentation

- Ship operators
- Ship managers

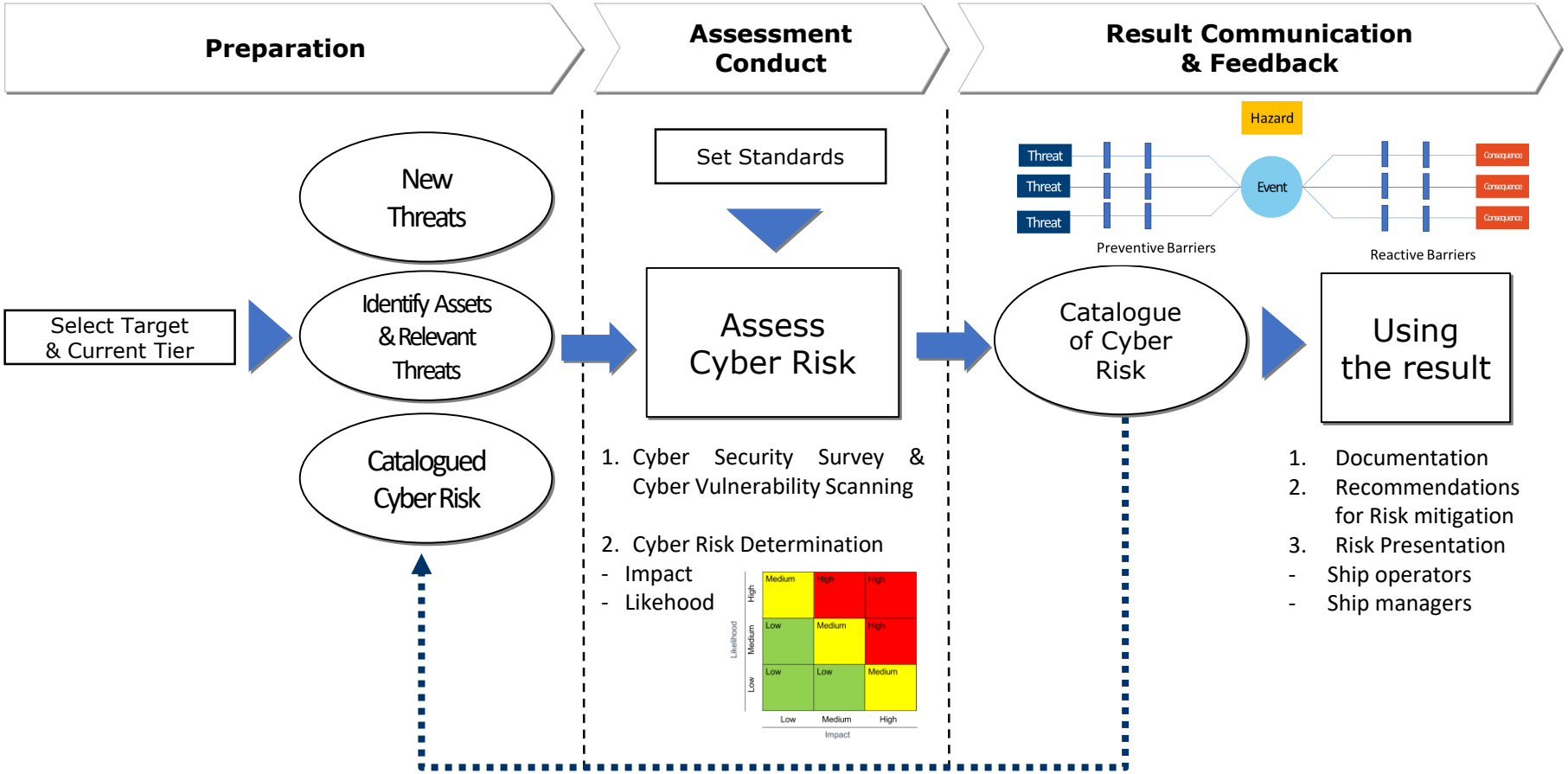
Result communication and feedback: The entity should document the results of every assessment and **provide appropriate recommendations**. Then, it is important that they **share it among the entity's operators and managers.**

Information | Action

** This cyber risk self assessment procedure is referred from the guidelines on maritime cybersecurity by KR, DNV-GL, Maritime Cyber Risk Management: An Experimental Ship Assessment(Boris Svilicic), and Cyber Threat Metrics(Mark Mateski)*

03. Proposals

① Include Cyber risk self assessment: Appendix



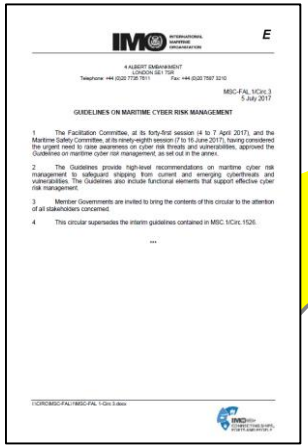
** This cyber risk self assessment procedure is referred from the guidelines on maritime cybersecurity by KR, DNV-GL, Maritime Cyber Risk Management: An Experimental Ship Assessment(Boris Svilicic), and Cyber Threat Metrics(Mark Mateski)*

03. Proposals

② Include the Guidelines in MSC.1/Circ.1371

MSC.1/Circ.1371, a List of codes, recommendations, guidelines and other safety- and security-related non-mandatory instruments

which is referred to in paragraph 1.2.3.2 of the ISM Code.



IMO E

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

MSC-FAL.1/Circ.3
5 July 2017

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.

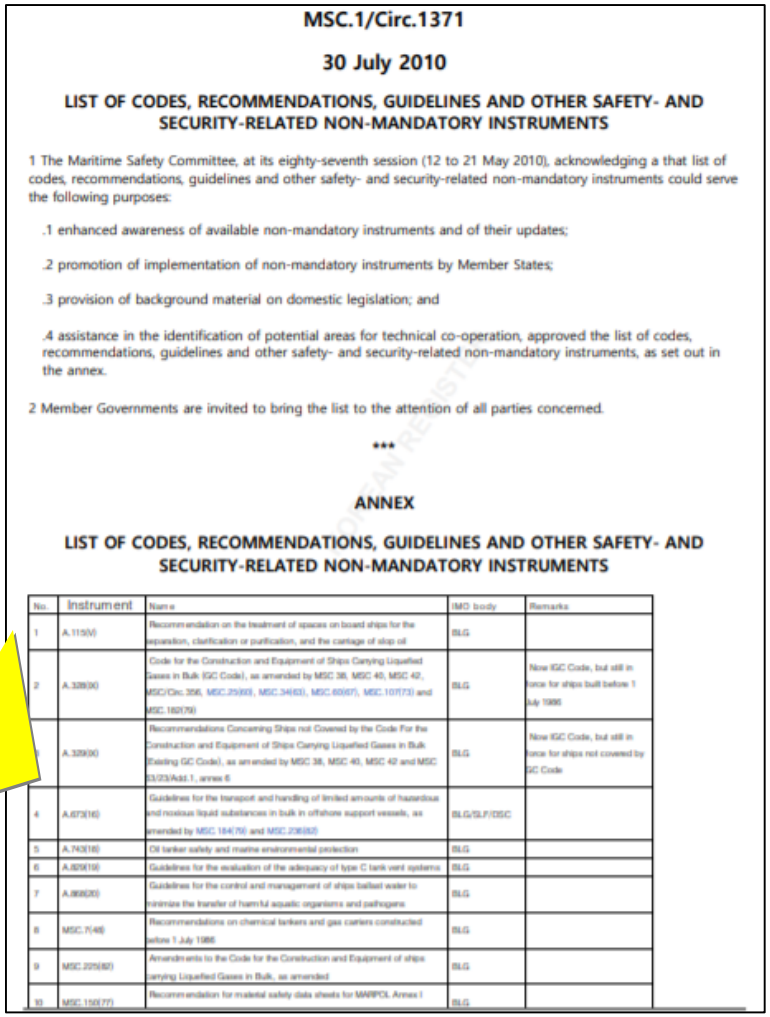
2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

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

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

...

I:\CIRC\MSC-FAL\MSC-FAL.1-Circ.3.docx



MSC.1/Circ.1371

30 July 2010

LIST OF CODES, RECOMMENDATIONS, GUIDELINES AND OTHER SAFETY- AND SECURITY-RELATED NON-MANDATORY INSTRUMENTS

1 The Maritime Safety Committee, at its eighty-seventh session (12 to 21 May 2010), acknowledging a that list of codes, recommendations, guidelines and other safety- and security-related non-mandatory instruments could serve the following purposes:

.1 enhanced awareness of available non-mandatory instruments and of their updates;

.2 promotion of implementation of non-mandatory instruments by Member States;

.3 provision of background material on domestic legislation; and

.4 assistance in the identification of potential areas for technical co-operation, approved the list of codes, recommendations, guidelines and other safety- and security-related non-mandatory instruments, as set out in the annex.

2 Member Governments are invited to bring the list to the attention of all parties concerned.

***

ANNEX

LIST OF CODES, RECOMMENDATIONS, GUIDELINES AND OTHER SAFETY- AND SECURITY-RELATED NON-MANDATORY INSTRUMENTS

No.	Instrument	Name	IMO body	Remarks
1	A.1115(V)	Recommendation on the treatment of spaces on board ships for the separation, clarification or purification, and the carriage of slop oil	BLG	
2	A.328(IX)	Code for the Construction and Equipment of Ships Carrying Liquefied Gases in Bulk (GC Code), as amended by MSC 38, MSC 40, MSC 42, MSC/Circ.356, MSC.25(60), MSC.34(63), MSC.60(67), MSC.107(73) and MSC.182(79)	BLG	New IGC Code, but still in force for ships built before 1 July 1986
3	A.329(IX)	Recommendations Concerning Ships not Covered by the Code For the Construction and Equipment of Ships Carrying Liquefied Gases in Bulk (Existing GC Code), as amended by MSC 38, MSC 40, MSC 42 and MSC 53/23/Add.1, annex 6	BLG	New IGC Code, but still in force for ships not covered by GC Code
4	A.673(16)	Guidelines for the transport and handling of limited amounts of hazardous and noxious liquid substances in bulk in offshore support vessels, as amended by MSC.164(78) and MSC.238(82)	BLG/SLF/DSC	
5	A.743(18)	Oil tanker safety and marine environmental protection	BLG	
6	A.829(19)	Guidelines for the evaluation of the adequacy of type C tank vent systems	BLG	
7	A.868(20)	Guidelines for the control and management of ships ballast water to minimize the transfer of harmful aquatic organisms and pathogens	BLG	
8	MSC.7(48)	Recommendations on chemical tankers and gas carriers constructed before 1 July 1986	BLG	
9	MSC.225(82)	Amendments to the Code for the Construction and Equipment of ships carrying Liquefied Gases in Bulk, as amended	BLG	
10	MSC.150(77)	Recommendation for material safety data sheets for MARPOL Annex I	BLG	

Include the revised MSC-FAL.1/Circ.3

③ Amend ISM Code

PART A - IMPLEMENTATION

1 GENERAL

1.2.2 Safety management objectives of the Company should, inter alia:

.1 provide for safe practices in ship operation, a safe working environment, **and preventive measures against cyber incidents or threats**;

이건 레퍼런스 부분이다

04. Conclusion

Conclusion

References

IMO Document

[1]Resolution MSC.428(98)
[2]MSC-FAL.1-Circ.3
[3]MSC.1/Circ.1371
[4-11]MSC 94/4/1, MSC 96/INF.4, MSC 96/4/2, MSC 97/4, MSC98/23, MSC 101/4/1, MSC 101/4/4, MSC 101/24

Report

[12]BIMCO, Safety at Sea: cyber security whitepaper 2019
[13]Guidelines on cyber security onboard ships version 3.
[14]DNVGL, RP-0496, Cyber security resilience management for ships and mobile offshore units in operation
[15]DNV-GL, Cyber security capabilities of control system components
[16]Deloitte, 사이버보안과 내부 감사의 역할
[17]Boris Svilicic et al, Maritime Cyber Risk Management: An Experimental Ship Assessment
[18]Mark Mateski, Cyber Threat Metrics
[19]United States National Institute of Standards (NIST), The Cybersecurity Framework Version 1.1.
[20]KR, Guidelines for the Maritime Cybersecurity Management System
[21]KR, 해상 사이버보안 관리 시스템 지침
[22]한국정보보호진흥원, 사이버보안을 위한 국가프레임워크 개발: 이슈와 대안 분석 2006.6
[23]이용찬, Improving cyber security awareness in maritime transport: a way forward
[24]CIS, CIS-Controls version 7.1
[25]U.S. DHS Transportation Systems Sector Cybersecurity Framework Implementation Guidance
[26] USCG, Marine Sfatety Alert: Cyber Incidnet Exposes Potential Vulnerabilities Onboard Commercial Vessels, July 8, 2019

Thank you

Proposals for Effective Cyber Risk Management

Presented by Mersea