Tasneef

هيئة الإمارات للتصنيف
Emirates Classification Society

Amendments to the "Guide for the Assessment of Cyber Resilience of Ships and Offshore Units"

GUI/038/AMN/01

Effective from 1 October 2020

INDEX

1 GENERAL

1.1 Introduction

The IMO Resolution MSC.428(98), noting the objectives of the ISM Code, 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 and 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.

1.2 Aim and purpose

The aim of this guide is to provide indications for the assessment of the resilience of ships and offshore units to cyber incidents and management of related risks to safeguard shipping from current and emerging cyber threats and vulnerabilities.

The purpose of this Guide is to provide an instrument for proper management of cyber-related risk, in line with the recommendations contained in the IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management" and the IMO MSC-FAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management".

1.3 Scope of applicability

This Guide applies to ships and offshore units having on-board computer based systems (CBS) connected in networks, which can be vulnerable to cyber events potentially compromising the confidentiality, integrity and/or availability of information managed by means of such systems and networks.

The cyber events considered in this Guide are intentional or accidental unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in on-board CBS or transported by the networks connecting such systems (cyber incidents).

It also applies to ship owners or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the ship owner (Company), and in particular to personnel and organizational units involved at all levels in the management of cyber-related risks.

1.4 Reference regulations, guidelines, standards

The following international or industrial standards, regulations and guidelines may be considered as a technical background for this Guide:

- IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management", June 2017
- IMO MSC-FAL.1/Circ.3, "Guidelines on Maritime Cyber Risk Management", July 2017
- NIST "Framework for Improving Critical Infrastructure Cybersecurity", version 1.1, April 2018
- "The Guidelines on Cyber Security On-board Ships", v3, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, December 2018
- "International Safety Management Code", 2014
- ISA/IEC 62443 Series, International Society of Automation.

2 COMPANY-LEVEL PROVISIONS

For the assessment of resilience of Companies to cyber incidents and for their management of cyber-related risks in accordance with the objectives and functional requirements of the ISM Code, the following should be taken into account.

For the verification of provisions in this section, the checklist in Appendix 1 should be used.

2.1 Policy

The Company's policy should be modified, extending its ISM management objectives with the inclusion of cyber security issues and the necessary measures for the mitigation of cyber-related risks.

2.2 Responsibility

The Company should designate a responsible ashore for the management and protection against cyber-related risks, to provide assistance to the ship responsible persons.

2.3 Compliance

The Company should take into account applicable codes, guidelines and recommendations from IMO, Administrations, classification societies and maritime industry organizations; they constitute a basis for risk assessment and the Company's SMS.

2.4 Risk Assessment

The Company should provide a risk assessment (RA) and should identify cyber-related risks, safeguards and responsibilities, taking in due consideration applicable rules, guidelines and recommendations.

In the development of the RA, the differences between Operational Technology (OT) and Information Technology (IT) Systems should be taken into account. To this purpose, MSC-FAL.1/Circ.3 par. 2.1.2 and "The Guidelines on Cyber Security On-board Ships" par. 1.1 should be considered as reference.

The following functional elements, that support effective cyber-related risk management, should be addressed appropriately (see MSC-FAL.1/Circ.3 par 3.5 and the NIST "Framework for Improving Critical Infrastructure Cybersecurity"; for details on specific aspects to be taken into account see also “The Guidelines on Cyber Security On-board Ships”, Annex 2):

- Identify: Define personnel roles and responsibilities for cyber-related risk management and identify the systems, assets, data and capabilities that, when affected by a cyber incident, pose risks to ship operations.
- Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber incident and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect a cyber incident in a timely manner.
- Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber incident.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident.

A systematic Hazards Identification (HAZID) of cyber-related potential hazards and a Resource Identification (RESID) of either internal or external resources (for example manufacturers and technicians for the protection of OT and IT systems that could be involved) potentially at risk should be done.

2.5 Results of Risk Assessment

The Company should develop procedures and risk mitigation measures based on the results of risk assessment. These should be effectively communicated to the crew, also taking into account appropriate roles and responsibilities and possible restrictions on dissemination of information.

2.6 Master

The Company should clearly indicate in the SMS the procedures in charge to the ship's Master, taking however into account that, when considering cyber-related risks, some tasks can be not solely the responsibility of the Master but distributed among other seafarers with defined responsibility ashore and aboard.

2.7 Support Offices

The Company should be prepared to provide qualified support to the Master from shore offices in order to implement the measures and procedures envisaged for cyber-related risk management, at least providing support on how to respond to and recover from a cyber incident.

2.8 Familiarization and training

The Company should provide suitable means to the crew on-board and the staff ashore for the familiarization with the tools and procedures for cyber-related risk management. Familiarization and training should be periodically refreshed. The SMS should contain a training plan and describe the measures to determine training needs for seafarers and related shore staff according to roles and positions.

2.9 Emergency

The Company should include in the SMS a "cyber security contingency plan" and should provide exercises, simulations and training to prepare for emergency actions. Plans should at least include measures to respond to a meaningful set of possible cyber incidents, a description of their possible consequences and the necessary recovery measures.

2.10 Reports

The Company should establish procedures for the prompt reporting of cyber incidents, near misses and other relevant events to the managers of the Company. These procedures should be specified in the SMS manual.

2.11 Maintenance of equipment

The Company should include in the planned maintenance systems the activities to be carried out periodically and identified in the RA as mitigation measures for cyber-related risks. These activities should be duly monitored and documented.

2.12 Documentation

In case the mitigation measures include the management of sensitive data or reserved documents, the Company should implement specific measures for the management of such data and documents, e.g. limiting the access thereto to accredited persons.

2.13 Verification

The Company should carry out internal audits on-board and ashore at intervals not exceeding twelve months to verify whether cyber-related risk management is duly implemented and continuously updated.

2.14 Evaluation

The Company should verify and evaluate regularly the safety management system, focusing on the correct implementation and effectiveness of cyber-related risk management, qualification of auditors with regard to cyber-related matters, corrective and preventive actions on deficiencies found.

2.15 Continuous improvement

The Company should take into account the continuously changing scenarios of cyber-related risks and the weaknesses identified in its systems and ensure the continuous updating of the risk assessment and SMS system.

3 SHIP-LEVEL PROVISIONS

For cyber-risk management on ships having on-board CBS connected in networks, which can be vulnerable to cyber incidents potentially compromising the confidentiality, integrity and/or availability of information managed by means of such systems and networks, the following should be taken into account. The extent and level of application of the following provisions should take into account factors related to:

a) The ship as a whole, like service notation, navigation notation, overall level of digitalization on-board, extension and interconnection of different networks, etc.

b) Functions provided by the CBS, e.g. Control, Alarm, Monitoring, Communication etc., in decreasing order of priority.

c) Type of service provided by the system the CBS is part of, e.g. Essential, Auxiliary Commodity or Entertainment services, in decreasing order of priority. In defining priority, availability of essential systems and of systems to remain operational for the safe operation of the ship should be considered of highest priority. For OT systems, Cat.I, II and III as described in Tasneef Rules Pt.C Ch.3 Sec.3 Table 1 may also be used for prioritizing.

d) Severity of consequences of potential cyber incidents affecting the CBS, ranked e.g. as Negligible, Minor, Moderate, Major or Catastrophic. Failure Mode Effect and Criticality Analysis (FMECA) can be used to this purpose.

e) Likelihood of occurrence of cyber incidents affecting the CBS, ranked e.g. as High, Medium or Low. To this purpose, possible threats and countermeasures already in place should be identified for the systems under consideration.

3.1 Documentation

The documentation relevant to this section (see **Table 1**) should be provided to the Society either in the form of a single document, hereafter referred to as the ship's "Cyber Resilience Manual", or as separate documents.

The Company should keep the documentation up to date and in line with the changes made to the CBS on-board, network configuration, software updates and other maintenance activities.

The Society reserves the right to require additional information and/or documentation.

Table 1: Documentation to be submitted

Document	Submitted for
Inventory of computer based systems on-board and persons allowed to have access to the CBS on-board and network infrastructure	Information
Vulnerability and threat assessment	Information
Risk assessment	Approval
Protection safeguards	Information
Detection safeguards	Information
Response and recovery measures and procedures	Information
Test	Information
Maintenance	Information

3.2 Inventory

An inventory of the CBS on-board the ship and relevant networks should be provided by the Company, either as a separate document or as part of the Cyber Resilience Manual, retained on-board and made available to the Society for inspection.

The inventory should contain:

a) The list of computer based systems, subsystems and programmable devices on-board the ship, with a short description of technical features and specific function for each.

b) The category of each item identified in a), according to Tasneef Rules Pt C, Ch 3, Sec 3, Table
1. A map describing the topology of each digital network connecting the items identified in a), including the intended function of each item, the main features of each network (e.g. protocols used) and communication data flows in all intended operation modes.

c) A map describing the physical layout of each digital network connecting the items identified in a), including the physical location of the items on-board, the paths of network cables (for wired networks) or the position of wireless transmitters and receivers (for wireless networks), and the physical location of network access points.

d) The list of software application programs, operating systems (if any), firmware and other software components installed on each item identified in a), including version numbers, maintenance policy (e.g. on-site vs. remote, periodic vs. occasional, etc.) and responsible persons.

e) Maintenance policy (e.g. on-site vs. remote, periodic vs. occasional, etc.) of hardware and software components, including responsible persons and procedures.

The following CBS, if present on-board, should be included in the inventory:

OT Systems:

- Propulsion and Fuel Oil system
- Steering system

- Main source of electrical power
- Alarm Systems
- Control Systems
- Safety Systems
- Navigation Systems
- ESD (Emergency Shut Down) system
- Emergency source of electrical power
- UPS (Uninterruptable Power Supplies)
- Internal and external communication systems
- Fire extinguishing systems
- Safety centre control system (for passenger ships)
- Bilge and ballast systems
- Anti-heeling pumps
- Valves control and monitoring
- Power-operated watertight and semi-watertight doors (for passenger ships)
- Fire doors (for passenger ships)
- Flooding detection system (for passenger ships)
- Sanitation
- Grey Water system
- Refrigeration of food
- Lighting
- Ventilation and air conditioning
- Lifts (for passenger ships)
- Any other system whose disruption or functional impairing may pose risks at ship operation (e.g. LNG monitoring and control system, relevant gas detection system etc.)

IT systems:

- Specific Hotel services (for passenger ships) e.g. Laundry, Galley
- HVAC
- Ship Owner Network
- Performance monitoring systems
- Networks and devices used for update of data on on-board systems (e.g. ECDIS).

The systems, equipment and technology listed in “The Guidelines on Cyber Security On-board Ships”, Annex 1, should also be considered in the inventory.

An inventory of persons that are granted to have access to the CBS and network infrastructure, either on-board the ship or from other location, should be provided. The inventory should contain:

a) The names of persons granted to having access to CBS and network infrastructure, including seafarers, personnel internal to the Company and other personnel not part of the Company (e.g. Suppliers).
b) Their role and responsibility in the context of the system(s) they have access to, e.g. Administrator, Operator, Maintainer, etc. with a description of their permissions on relevant data and resources, e.g. read, write, modify, erase.
c) The access points they are allowed to access for connecting to the network(s), either on-board the ship or in other location.
d) The time period for which their access is granted.

An inventory of other persons having roles and/or responsibility in the management of CBS on-board and/or in ship’s cyber related risk management should also be provided, with relevant description.

3.3 Vulnerability and threat assessment

A vulnerability assessment and a threat assessment should be carried out for the systems exposed to higher risk. The vulnerability assessment should be carried out at least for all OT systems of Cat II and III and systems connected thereto. The vulnerability and threat assessments should also be carried out for IT systems connected to OT systems, either permanently or temporarily, e.g. during maintenance of CBS on-board.

The vulnerability assessment and the threat assessment should be carried out by personnel with specific skills and demonstrated expertise. The level of investigation and extension/depth of tests should be proportional to the risk level of the system under examination.

Typical vulnerabilities should be identified by means of specific investigation tools and techniques and also taking into account available knowledge bases and/or audits of similar systems. A scoring system may be used to communicate the characteristics and impacts of vulnerabilities, and produce a numerical score reflecting their severity.

Threats should be identified taking into account at least:

a) The vulnerabilities found on systems.
b) Potential threat actors, including e.g. nation states; terrorists; cyber criminals; organized crime; competitors; activist groups; careless, disgruntled or malicious insiders; cyber vandals; opportunists; unaware passengers; and others.
c) Different purposes and interests for each possible threat actor.
d) Their offensive capability and the probability of an attack, either intentional or accidental, that may depend on the ship type, operation, navigation, cargo, etc.
e) Available knowledge bases and/or audits of similar systems.

The outcomes of vulnerability assessment and threat assessment should be made available to the Company and provided to the Society, either as a separate document or as part of the Cyber Resilience Manual, retained on-board and made available to the Society for inspection.

3.4 Risk assessment

A risk assessment should be carried out by the Company in cooperation with other interested stakeholders for the systems identified in the inventory. Systems can be grouped in homogeneous sets or by categories (Cat. I, II or III).

The risk assessment should consider likelihood of occurrence (probability) vs. safety and security impacts (severity) resulting from the exposure or exploitation of vulnerabilities and threats identified.

The outcomes of risk assessment should be made available to the Company and provided to the Society, either as a separate document or as part of the Cyber Resilience Manual, retained on-board and made available to the Society for inspection.

3.5 Protection safeguards

3.5.1 General

Protection safeguards should be implemented by the Company aimed to prevent the occurrence of adverse cyber incidents on on-board CBS and networks.

Protection safeguards should be clearly described, either in a separate document or as part of the Cyber Resilience Manual, that should be provided to the Society, retained on-board and made available to the Society for inspection.

3.5.2 Access control

A policy for access control to CBS on-board should be established and implemented by the Company, aimed at limiting the access to authorized users, processes or devices, and for authorized activities.

The access control policy should cover at least the following aspects:

a) Management of credentials (e.g. usernames and passwords), including periodical expiration and non-repetition; use of administrative profiles (e.g. adoption of least-privilege policy); use of credentials available to groups of persons (e.g. forbid one common account for maintenance of all systems).

b) Management of physical access to all on-board network access points or standalone devices, including access recording logs and control of connection ports and drives for removable storage devices.

c) Management of remote access to on-board systems, including enforced access control methods (e.g. multi-factor authentication), limited and explicitly agreed time windows for remote access, etc.

d) Implementation of least-privilege policies

e) Bring-your-own-device (BYOD) management policy, including notification to users of the Acceptable Use Policy of on-board facilities.

Procedures for testing the actual and effective implementation of protection safeguards adopted should be clearly described in order to allow execution of such procedures e.g. during inspection and verification.

3.5.3 Network protection

Technical and procedural measures should be implemented by the Company for protecting the network, including, but not limited to:

a) Network segregation, in particular separation between OT and IT networks,

b) Firewalling,

c) Use of so-called de-militarized zones (DMZ)[(1)],

d) Selection/control of IP addresses,

e) Implementation of Intrusion Prevention Systems (IPS),

f) WiFi hardening,

g) Use of controlled Virtual Private Networks (VPN), etc. as applicable.

[(1)] A de-militarized zone can be defined as a network, either physical or logical, that provides an interface to an untrusted external network – usually the internet – while keeping the internal, private network – e.g. a ship's on-board network – separated and isolated form the external network.

3.5.4 Data protection

Devices used to store data used in CBS on-board should be appropriate for the intended use and suitable for the marine environment, according to relevant regulations, e.g. IEC Performance Standards.

A policy for the effective data security should be established and implemented, aimed at preserving the confidentiality, integrity and availability of data used by CBS on-board and relevant networks.

The data security policy should cover at least the following aspects:

a) Redundancy of storage devices to protect data in the case of a drive single failure, e.g. RAID storage or equivalent. Redundancy of storage devices is mandatory for data used for Cat. II or Cat. III OT systems.

b) Availability of spare compatible storage devices on-board.

c) Sanity check of removable/portable storage devices brought on-board the vessel against data corruption or malware infection before connection to on-board systems and networks.

d) Encryption for data at rest (stored) and data in transit (exchanged)

e) Integrity checks for data at rest and data in transit

f) Data backup procedures

g) Secure disposal of storage devices.

3.5.5 Awareness and training

Cybersecurity awareness education and training should be provided by the Company to the on-board personnel and possible other stakeholders to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Drills and training updates, or equivalent, should be provided aimed at maintaining and verifying the training.

An acceptable use policy of the cyber resources available on-board should be established by the Company and notified to persons other than on-board personnel having access to on-board networks (e.g. passengers).

3.6 Detection safeguards

3.6.1 General

Detection safeguards should be implemented by the Company aimed at a timely detection and identification of cyber incidents on on-board CBS and networks.

Roles relevant to security event monitoring should be assigned and procedures defined.

Detection safeguards should be described, either in a separate document or as part of the Cyber Resilience Manual that should be provided to the Society, retained on-board and made available to the Society for inspection.

3.6.2 Monitoring of normal operation

Means for the monitoring of CBS normal operations should be provided, based on an analysis of the system and network baseline operation and expected data flows.

Continuous and/or on-demand self-diagnostics should be available at least on OT systems of Cat. II and III and on IT systems connected to OT systems.

A description on how system or network abnormal operation can be detected should be provided, if not self-evident.

Connection quality and/or network performance monitoring tools should be available at least on networks connecting OT systems of Cat. II and III and on networks connecting IT systems to OT systems.

3.6.3 Real-time detection of cyber incidents

Intrusion Detection Systems (IDS) should be provided at least on networks with connection to shore or freely accessible access points.

Malicious code detection tools, e.g. antivirus, antimalware, etc., should be provided on systems connected to networks with connection to shore or freely accessible access points.

Means should be available to display the occurrence of cyber incidents in a timely, informative and unambiguous manner, including but not limited to attempts of unauthorized access to CBS, unauthorized maintenance, attempts to alter data or code, etc.

3.6.4 Offline auditing

Means for recording cyber incidents should be available, aimed at allowing the examination of all the events detected by the above listed safeguards on a given period of time (e.g. one week, one month,…).

Event log auditing should be carried out, either periodically or after detection of cyber incidents [1.4.2], by personnel with specific skills and demonstrated expertise.

A plan for periodic vulnerability scans and security audits should be defined. The plan should consider also the repetition of vulnerability scans after maintenance activities, or changes in the network configuration, or in CBS, where deemed necessary.

3.7 Response and recovery measures and procedures

3.7.1 General

Response and recovery measures and procedures should be implemented aimed to take appropriate actions regarding detected cyber incidents on on-board CBS and networks.

Response measures and procedures should be described in a separate document or in a dedicated section of the Cyber Resilience Manual that should be provided to the Society, retained on-board and made available to the Society for inspection.

3.7.2 Response and recovery plan

A response plan for the effective and timely response to possible cyber incidents should be provided, aimed at limiting as much as possible the extension and duration of consequences and restore the relevant services to the ship.

The response and recovery plan should cover at least the following aspects:

a) Clear description of alerts for a timely acknowledgement of cyber incidents.
b) Step-by-step procedures for the isolation, exclusion, backup, replacement by redundant system, manual/local operation, shutdown, reset, restart or other measure to be adopted for the CBS and/or networks affected by the cyber incident
c) Step-by-step procedures for the recovery of data managed by CBS and/or networks affected by the cyber incident
d) Assignment of roles, responsibilities and tasks to on-board personnel involved in the response procedures
e) Instruction for timely and effective information to and communication with responsible personnel
f) Processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems. Reporting should include also the results of the measure taken and collection of relevant information which may serve as evidence and support a continuous improvement process.

3.8 Test

Procedures for verifying the actual and effective implementation of safeguards and measures described in paragraphs above should be clearly described in relevant documentation in order to allow the Society to execute such procedures during inspection. The Society may require additional or alternative tests if deemed necessary.

3.9 Maintenance

The Company shall establish procedures for the maintenance of CBS on-board, e.g. software updates. The following aspects shall be covered:

a) Roles and responsibilities: personnel involved in maintenance activities
b) Initiation: the circumstances, or events, that may trigger a maintenance activity
c) Planning: a description of the activities to be carried out, conditions to be met and arrangements to be made for the maintenance to be performed.
d) Execution: a description of how the maintenance activity is actually carried out.
e) Test: a description of acceptance tests (Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), User Acceptance Tests (UAT), etc. as applicable) to be performed aimed at verifying the success of the maintenance activity. Acceptance tests shall include functional, regression and performance tests. An explanation of how to check the current software/firmware version installed on the CBS subject to maintenance should be also included.
f) After-service: how to provide information to the personnel responsible of or using the CBS subject to maintenance.
g) Rollback: a description of how to restore the CBS to a safe status in case of failure of the maintenance activity.

A record of maintenance activities shall be kept up to date. Acceptance tests results shall be recorded.

Maintenance procedures shall be documented in a separate document or in a dedicated section of the Cyber Resilience Manual that shall be provided to the Society, retained on-board and made available to the Society for inspection.

In case of major maintenance activities, the Company shall inform the Society. The Society reserves the right to verify the conditions for the maintenance of the statement of compliance to this Guide.

4 STATEMENT OF COMPLIANCE

4.1 General

Upon Company request and positive verification of documentation and of implementation of measures defined in this Guide, a Statement of Compliance to the recommendations given in this Guide is issued by Tasneef. The Statement of Compliance can be issued to:

- Shipowners/Companies only (using the whole Guide except section 3), or
- Ships/offshore units only (using the whole Guide except Section 2), or
- Both Shipowners/Companies and ships/offshore units (using the whole Guide).

Tasneef is to be promptly informed by the Company in the case of any changes occurring related to aspects which could influence the capacity to continue meeting the requirements of this Guide, and reserves the right to perform additional audits if the changes communicated are considered particularly relevant as regards maintenance of compliance with the requirements of this Guide.

4.2 Validity

The statement validity will expire in five years, and is to be confirmed by a yearly follow-up audit.

The statement validity will be suspended in accordance with the “General contract conditions governing system, product and personnel certification” and also

- upon Company request or
- in case the Company does not allow the annual audits to be carried out when due
- in case the Company has not met the deadline established for corrective action communication
- as a consequence of a major non conformity not resolved within the time limit established or
- as a consequence of numerous observations affecting the proper functioning of the cyber-related risk management process not resolved within the time limit established or
- in case the Company has carried out major restructuring without informing Tasneef of these changes or
- in case the Company has made significant changes to the cyber system which have not been accepted by Tasneef or
- in case of any justified and serious complaints received by Tasneef are confirmed.

4.3 Suspension

Suspension is notified in writing, stating the conditions for reinstatement of validity the statement and the deadline by which these are to be fulfilled.

4.4 Reinstatement

In case of suspension, to reinstate the statement validity, an additional audit is to be carried out.

Reinstatement is dependent on verification that the shortcomings, which led to suspension, have been eliminated.

Checklist for the verification of compliance to the “Guide for the Assessment of Cyber Resilience of Ships and Offshore Units” (GUI38) Section 2 “COMPANY-LEVEL PROVISIONS”

Introduction

The IMO Resolution MSC.428(98), noting the objectives of the ISM Code, 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 and 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.

The purpose of GUI38 is to provide an instrument for proper management of cyber-related risk, in line with the recommendations contained in the IMO Resolution MSC.428(98) “Maritime Cyber Risk Management in Safety Management” and the IMO MSC-FAL.1/Circ.3 “Guidelines on Maritime Cyber Risk Management”.

Such recommendations are also reflected in Circular S.G. 155-2019 published by the Italian Ministero delle Infrastrutture e dei Trasporti, Comando generale del Corpo delle capitanerie di porto Reparto 6° - Ufficio 2° - Sezione 1ª “SICUREZZA DELLA NAVIGAZIONE” on cyber risk management.

Section 2 of GUI38 contains provisions to be applied at Company level for the assessment of resilience of Companies to cyber incidents and for their management of cyber-related risks, in line with the objectives and functional requirements of the ISM Code, IMO MSC428(98), IMO MSC-FAL.1/Circ.3 and MIT S.G. 155-2019.

Checklist

Provision	**Test**	**Result**	**Notes**
2.1 Policy The Company's policy should be modified, extending its ISM management objectives with the inclusion of cyber security issues and the necessary measures for the mitigation of cyber-related risks.	Does the Company provide evidence of having extended its ISM management objectives with the inclusion of cyber security issues and necessary measures for the mitigation of cyber related risks? *This evidence can be provided showing how ISM objectives have been updated, how risks related to cyber issues have been duly considered and what mitigation measures have been planned.*		
2.2 Responsibility The Company should designate a responsible ashore for the management and protection against cyber-related risks, to provide assistance to the ship responsible persons.	Does the Company have a responsible person ashore for the management and protection against cyber-related risks? *Please indicate the name of responsible person and check that his/her role inside the Company’s hierarchy allows making decisions and*		

Provision	**Test**	**Result**	**Notes**
	taking actions according to his/her task, e.g. having access to data, information and resources that might be needed for providing assistance to ship responsible persons		
	Does the Company have sufficient personnel and/or resources for a prompt and continuous (e.g. 24/7) assistance to ships? *Check how many persons are involved in the provision of assistance service and if their organization is compatible with the intended coverage, both geographically and in time*		
2.3 Compliance The Company should take into account applicable codes, guidelines and recommendations from IMO, Administrations, classification societies and maritime industry organizations; they constitute a basis for risk assessment and the Company's SMS.	Has the Company duly taken into account applicable codes, guidelines and recommendations from IMO, Administrations, classification societies and maritime industry organizations? *Examples are:* *IMO MSC 428(98)* *IMO MSC-FAL.1/Circ.3* *ISM Code* *MIT S.G. 155-2019* *Tasneef GUI38-ENG* *BIMCO Guidelines* *Etc.*		
2.4 Risk Assessment The Company should provide a risk assessment and should identify cyber-related risks, safeguards and responsibilities, taking in due consideration applicable rules, guidelines and recommendations.	Has the Company carried out a risk assessment aimed at identifying cyber-related risks? *Check also if the risk assessment has been carried out according to recognized practices and methodologies*		
In the development of the RA, the differences between Operational Technology (OT) and Information Technology (IT) Systems should be taken into account.	In the risk assessment, have the differences between OT and IT been duly taken into account? *According to IMO MSC-FAL.1/Circ.3, information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.*		

Provision	Test	Result	Notes
	Check if IT and OT systems have been duly identified in the RA.		
The following functional elements, that support effective cyber-related risk management, should be addressed appropriately: - Identify - Protect - Detect - Respond - Recover	In Company's risk management, have the five elements (Identify, Protect, Detect, Respond, Recover) been duly addressed? *To check the above, the following elements can be verified in the Company's risk management:* ***Identify** - an inventory of the following items has been done:* - *assets that may be subject to cyber risks have been done;* - *personnel operating on such systems, and their roles and responsibilities;* - *Data at risk;* ***Protect** – at least the following measures have been adopted:* - *Training and drills at all levels of Company's hierarchy on cybersecurity risks* - *Control of physical access to IT and OT systems* - *Password management* - *Least privilege policy* - *Network segmentation and separation* - *Firewalls and antivirus* - *Data encryption and integrity checks* - *Backup policies* - *Secure disposal of storage devices* ***Detect** – at least the following measures have been adopted:* - *Continuous monitoring of IT and OT systems' operation by means of firewalls and antivirus with real-time scanning and alert* - *Periodical sanity checks of hardware, software and data* - *Network intrusion detection systems* ***Respond** – The Company has a response plan for the effective and*		

Provision	Test	Result	Notes
	timely response to possible cyber incidents, aimed at limiting as much as possible the extension and duration of consequences of a cyber incident. The plan should include: • *Clear description of alerts for a timely acknowledgement of cyber incidents.* • *Step-by-step procedures for the isolation of cyber incident* • *Assignment of roles, responsibilities and tasks* • *Instruction for timely and effective information and communication with responsible personnel* ***Recover** - The Company has a recovery plan to restore cyber systems impacted by a cyber incident. The plan should include:* • *Step-by-step procedures for the replacement of damaged systems, shutdown, reset, restart or other measure to be adopted* • *Step-by-step procedures for the recovery of data and/or networks affected by the cyber incident* • *Assignment of roles, responsibilities and tasks*		
A systematic Hazards Identification (HAZID) of cyber-related potential hazards and a Resource Identification (RESID) of either internal or external resources (for example manufacturers and technicians for the protection of OT and IT systems that could be involved) potentially at risk should be done.	Has the Company carried out a HAZID and a RESID of either internal or external resources potentially subject to cyber risk? *Check if HAZID and RESID have been included in the RA and what methodology or guideline has been followed.*		
2.5 Results of Risk Assessment The Company should develop procedures and risk mitigation measures based on the results of risk assessment. These should be effectively communicated to the crew, also taking into account appropriate roles and	Has the Company effectively communicated the risk mitigation measures to its personnel on board and ashore, according to their roles and responsibilities? *Training of personnel, courses and internal communications should be demonstrated. Documentation should be provided witnessing specific skills*		

Provision	Test	Result	Notes
responsibilities and possible restrictions on dissemination of information.	*and/or qualification of personnel with responsibilities*		
2.6 Master The Company should clearly indicate in the SMS the procedures in charge to the ship's Master, taking however into account that, when considering cyber-related risks, some tasks can be not solely the responsibility of the Master but distributed among other seafarers with defined responsibility ashore and aboard.	Are the procedures for cyber risk management in charge to the ship's Master and other seafarers clearly indicated in relevant documentation? *Relevant documentation should be available.*		
2.7 Support Offices The Company should be prepared to provide qualified support to the Master from shore offices in order to implement the measures and procedures envisaged for cyber-related risk management, at least providing support on how to respond to and recover from a cyber incident.	Is the Company prepared to provide qualified support to the Master from shore offices in order to implement the measures and procedures envisaged for cyber risk management? *To verify this, at least the following should be checked:* • *Relevant roles and responsibilities have been assigned* • *Sufficient personnel and resources are available to provide support (e.g. worldwide, 24/7, …) according to the Company's needs* • *The Company has suitable network and communication infrastructure to ensure sufficient quality of service*		
2.8 Familiarization and training The Company should provide suitable means to the crew on-board and the staff ashore for the familiarization with the tools and procedures for cyber-related risk management. Familiarization and training should be periodically refreshed. The SMS should contain a training plan and describe the measures to determine training needs for seafarers	Does the Company provide suitable means to the crew on-board and the staff ashore for the familiarization with the tools and procedures for cyber risk management? *The Company's training plan should be checked at least for the following:* • *The personnel participating to the training activities* • *The frequency of refresher courses* • *The contents of training and means for the verification of attendees' proficiency*		

Provision	Test	Result	Notes
and related shore staff according to roles and positions.			
2.9 Emergency The Company should include in the SMS a "cyber security contingency plan" and should provide exercises, simulations and training to prepare for emergency actions. Plans should at least include measures to respond to a meaningful set of possible cyber incidents, a description of their possible consequences and the necessary recovery measures.	Does the Company have a cyber security contingency plan, providing exercises, simulations and training to prepare for emergency actions? *The Company's contingency plan should be checked at least for the following:* • *The personnel involved in exercises and/or simulations* • *The frequency of refresher training, exercises and simulations* • *The means for the verification of attendees' proficiency and effectiveness of emergency procedures*		
2.10 Reports The Company should establish procedures for the prompt reporting of cyber incidents, near misses and other relevant events to the managers of the Company. These procedures should be specified in the SMS manual.	Does the Company have established procedures, specified in the SMS manual, for reporting cyber incidents, near misses and other relevant events? *Possibly, samples of such reports on past events could be inspected, if available*		
2.11 Maintenance of equipment The Company should include in the planned maintenance systems the activities to be carried out periodically and identified in the RA as mitigation measures for cyber-related risks. These activities should be duly monitored and documented.	Are the activities identified in the RA as mitigation measures for cyber related risks and carried out periodically included in the Planned Maintenance System and duly monitored and documented? *This can be checked in the same way as for other maintenance activities*		
2.12 Documentation In case the mitigation measures include the management of sensitive data or reserved documents, the Company should implement specific measures for the management of such data and documents, e.g. limiting the access thereto to accredited persons.	For mitigation measures implying management of sensitive data or reserved documents, does the Company implement specific measures? *Check roles and responsibilities of personnel having access to such data and documents; check also measures for controlling access to such data and documents (e.g. management of access credentials such as passwords –*		

Appendix 1

Provision	Test	Result	Notes
	who has such credentials, how credentials are managed…)		
2.13 Verification The Company should carry out internal audits onboard and ashore at intervals not exceeding twelve months to verify whether cyber-related risk management is duly implemented and continuously updated.	Does the Company carry out internal audits onboard and ashore at intervals not exceeding twelve months? *Evidence should be provided by means of relevant documentation. Possibly, the contents of audits should be checked to verify their effectiveness concerning correct implementation of cyber risk management*		
2.14 Evaluation The Company should verify and evaluate regularly the safety management system, focusing on the correct implementation and effectiveness of cyber related risk management, qualification of auditors with regard to cyber-related matters, corrective and preventive actions on deficiencies found.	Does the Company regularly verify and evaluate its safety management system focusing on the correct implementation of cyber related risk management, qualification of auditors, corrective and preventive actions? *Evidence should be provided by means of relevant documentation*		
2.15 Continuous improvement The Company should take into account the continuously changing scenarios of cyber-related risks and the weaknesses identified in its systems and ensure the continuous updating of the risk assessment and SMS system.	Does the Company ensure the continuous updating of the risk assessment and SMS system, taking into account the continuously changing scenarios of cyber related risk and the weaknesses identified in its systems? *Evidence should be provided by means of relevant documentation. If available, evidence should also be given on how occurred cyber incidents have been investigated and countermeasures updated for a continuous improvement of cyber risk management*		