Tasneef®

Life Environmentally Optimized

Guide for the Assessment of Cyber Resilience of Ships and Offshore Units

Effective from 1 April 2020

Emirates Classification Society (Tasneef)
CI TOWER 17th Floor,
Corniche Road
Abu Dhabi, United Arab Emirates

Phone (+971) 2 692 2333
Fax (+971) 2 445 433
P.O. Box. 111155
info@tasneef.ae

GENERAL CONDITIONS

Definitions:

"*Administration*" means the Government of the State whose flag the Ship is entitled to fly or under whose authority the Ship is authorised to operate in the specific case.

"IACS" means the International Association of Classification Societies.

"*Interested Party*" means the party, other than the Society, having an interest in or responsibility for the Ship, product, plant or system subject to classification or certification (such as the owner of the Ship and his representatives, the ship builder, the engine builder or the supplier of parts to be tested) who requests the Services or on whose behalf the Services are requested.

"*Owner*" means the registered owner, the ship owner, the manager or any other party with the responsibility, legally or contractually, to keep the ship seaworthy or in service, having particular regard to the provisions relating to the maintenance of class laid down in Part A, Chapter 2 of the Rules for the Classification of Ships or in the corresponding rules indicated in the specific Rules.

"Rules" in these General Conditions means the documents below issued by the Society:

(i) Rules for the Classification of Ships or other special units;
(ii) Complementary Rules containing the requirements for product, plant, system and other certification or containing the requirements for the assignment of additional class notations;
(iii) Rules for the application of statutory rules, containing the rules to perform the duties delegated by Administrations;
(iv) Guides to carry out particular activities connected with Services;
(v) Any other technical document, as for example rule variations or interpretations.

"*Services*" means the activities described in Article 1 below, rendered by the Society upon request made by or on behalf of the Interested Party.

"Ship" means ships, boats, craft and other special units, as for example offshore structures, floating units and underwater craft.

"*Society*" or *"TASNEEF"* means Tasneef and/or all the companies in the Tasneef Group which provide the Services.

"*Surveyor*" means technical staff acting on behalf of the Society in performing the Services.

Article 1

1.1. The purpose of the Society is, among others, the classification and certification of ships and the certification of their parts and components. In particular, the Society:
(i) sets forth and develops Rules;
(ii) publishes the Register of Ships;
(iii) issues certificates, statements and reports based on its survey activities.

1.2. The Society also takes part in the implementation of national and international rules and standards as delegated by various G overnments.

1.3. The Society carries out technical assistance activities on request and provides special services outside the scope of classification, which are regulated by these general conditions, unless expressly excluded in the particular contract.

Article 2

2.1. The Rules developed by the Society reflect the level of its technical knowledge at the time they are published. Therefore, the Society, although committed also through its research and development services to continuous updating of the Rules, does not guarantee the Rules meet state-of-the-art science and technology at the time of publication or that they meet the Society's or others' subsequent technical developments.

2.2. The Interested Party is required to know the Rules on the basis of which the Services are provided. With particular reference to Classification Services, special attention is to be given to the Rules concerning class suspension, withdrawal and reinstatemen t. In case of doubt or inaccuracy, the Interested Party is to promptly contact the Society for clarification.
The Rules for Classification of Ships are published on the Society's website: www.tasneef.ae.

2.3. The Society exercises due care and skill:
(i) in the selection of its Surveyors
(ii) in the performance of its Services, taking into account the level of its technical knowledge at the time the Services are performed.

2.4. Surveys conducted by the Society include, but are not limited to, visual inspection and non-destructive testing. Unless otherwise required, surveys are conducted through sampling techniques and do not consist of comprehensive verification or monitoring of the Ship or of the items subject to certification. The surveys and checks made by the Society on board ship do not necessarily require the constant and continuous presence of the Surveyor. The Society may also commission laboratory testing, underwater inspection and other checks carried out by and under the responsibility of qualified service suppliers. Survey practices and procedures are selected by the Society based on its experience and knowledge and according to generally accepted technical standards in the sector.

Article 3

3.1. The class assigned to a Ship, like the reports, statements, certificates or any other document or information issued by the Society, reflects the opinion of the Society concerning compliance, at the time the Service is provided, of the Ship or product subject to certification, with the applicable Rules (given the intended use and within the relevant time frame).
The Society is under no obligation to make statements or provide information about elements or facts which are not part of th e specific scope of the Service requested by the Interested Party or on its behalf.

3.2. No report, statement, notation on a plan, review, Certificate of Classification, document or information issued or given as p art of the Services provided by the Society shall have any legal effect or implication other than a representation that, on the basis of the checks made by the Society, the Ship, structure, materials, equipment, machinery or any other item covered by such document or information meet the Rules. Any such document is issued solely for the use of the Society, its committees and clients or other duly authorised bodies and for no other purpose. Therefore, the Society cannot be held liable for any act made or document issued by other parties on the basis of the statements or information given by the Society. The validity, application, meaning and interpretation of a Certificate of Classification, or any other document or information issued by the Society in connection with its Services, is governed by the Rules of the Society, which is the sole subject entitled to make such interpretation. Any disagreement on technical matters between the Interested Party and the Surveyor in the carrying out of his functions shall be raised in writing as soon as possible with the Society, which will settle any divergence of opinion or dispute.

3.3. The classification of a Ship, or the issuance of a certificate or other document connected with classification or certificati on and in general with the performance of Services by the Society shall have the validity conferred upon it by the Rules of the Society at the time of the assignment of class or issuance of the certificate; in no case shall it amount to a statement or warranty of seaw orthiness,

structural integrity, quality or fitness for a particular purpose or service of any Ship, structur e, material, equipment or machinery inspected or tested by the Society.

3.4. Any document issued by the Society in relation to its activities reflects the condition of the Ship or the subject of certifi cation or other activity at the time of the check.

3.5. The Rules, surveys and activities performed by the Society, reports, certificates and other documents issued by the Society are in no way intended to replace the duties and responsibilities of other parties such as Governments, designers, ship builders, manufacturers, repairers, suppliers, contractors or sub-contractors, Owners, operators, charterers, underwriters, sellers or intended buyers of a Ship or other product or system surveyed.

These documents and activities do not relieve such parties from any fulfilment, warranty, responsibility, duty or obligation (also of a contractual nature) expressed or implied or in any case incumbent on them, nor do they confer on such parties any right, claim or cause of action against the Society. With particular regard to the duties of the ship Owner, the Services undertaken by the Society do not relieve the Owner of his duty to ensure proper maintenance of the Ship and ensure seaworthiness at all times. Likewise, t he Rules, surveys performed, reports, certificates and other documents issued by the Society are intended neither to guarantee the buyers of the Ship, its components or any other surveyed or certified item, nor to relieve the seller of the duties arising out of the law or the contract, regarding the quality, commercial value or characteristics of the item which is the subject of transaction.

In no case, therefore, shall the Society assume the obligations incumbent upon the above-mentioned parties, even when it is consulted in connection with matters not covered by its Rules or other documents.

In consideration of the above, the Interested Party undertakes to relieve and hold harmless the Society from any third party claim, as well as from any liability in relation to the latter concerning the Services rendered.

Insofar as they are not expressly provided for in these General Conditions, the duties and responsibilities of the Owner and Interested Parties with respect to the services rendered by the Society are described in the Rules applicable to the specific Service rendered.

Article 4

4.1. Any request for the Society's Services shall be submitted in writing and signed by or on behalf of the Interested Party. Such a request will be considered irrevocable as soon as received by the Society and shall entail acceptance by the applicant of all relevant requirements of the Rules, including these General Conditions. Upon acceptance of the written request by the Society, a contract between the Society and the Interested Party is entered into, which is regulated by the present General Conditions.

4.2. In consideration of the Services rendered by the Society, the Interested Party and the person requesting the service shall be jointly liable for the payment of the relevant fees, even if the service is not concluded for any cause not pertaining to the Society. In the latter case, the Society shall not be held liable for non-fulfilment or partial fulfilment of the Services requested. In the event of late payment, interest at the legal current rate increased by 1.5% may be demanded.

4.3. The contract for the classification of a Ship or for other Services may be terminated and any certificates revoked at the request of one of the parties, subject to at least 30 days' notice to be given in writing. Failure to pay, even in part, the fees due for Services carried out by the Society will entitle the Society to immediately terminate the contract and suspend the Services.

For every termination of the contract, the fees for the activities performed until the time of the termination shall be owed to the Society as well as the expenses incurred in view of activities already programmed; this is without prejudice to the right to compensation due to the Society as a consequence of the termination.

With particular reference to Ship classification and certification, unless decided otherwise by the Society, termination of the contract implies that the assignment of class to a Ship is withheld or, if already assigned, that it is suspended or withdrawn; any st atutory certificates issued by the Society will be withdrawn in those cases where provided for by agreements between the Society and the flag State.

Article 5

5.1. In providing the Services, as well as other correlated information or advice, the Society, its Surveyors, servants or agents operate with due diligence for the proper execution of the activity. However, considering the nature of the activities performed (see art. 2.4), it is not possible to guarantee absolute accuracy, correctness and completeness of any information or advice supplied. Express and implied warranties are specifically disclaimed.

Therefore, except as provided for in paragraph 5.2 below, and also in the case of activities carried out by delegation of Governments, neither the Society nor any of its Surveyors will be liable for any loss, damage or expense of whatever nature sustained by any person, in tort or in contract, derived from carrying out the Services.

5.2. Notwithstanding the provisions in paragraph 5.1 above, should any user of the Society's Services prove that he has suffered a loss or damage due to any negligent act or omission of the Society, its Surveyors, servants or agents, then the Society will pay compensation to such person for his proved loss, up to, but not exceeding, five times the amount of the fees charged for the specific services, information or opinions from which the loss or damage derives or, if no fee has been charged, a maximum of AED5,000 (Arab Emirates Dirhams Five Thousand only). Where the fees charged are related to a number of Services, the amount of the fees will be apportioned for the purpose of the calculation of the maximum compensation, by reference to the estimated time involved in the performance of the Service from which the damage or loss derives. Any liability for indirect or consequential loss, damage or expense is specifically excluded. In any case, irrespective of the amount of the fees charged, the maximum damages payable by the Society will not be more than AED5,000,000 (Arab Emirates Dirhams Five Millions only). Payment of compensation under this paragraph will not entail any admission of responsibility and/or liability by the Society and will be made without prejudice to the disclaimer clause contained in paragraph 5.1 above.

5.3. Any claim for loss or damage of whatever nature by virtue of the provisions set forth herein shall be made to the Society in writing, within the shorter of the following periods: (i) THREE (3) MONTHS from the date on which the Services were performed, or (ii) THREE (3) MONTHS from the date on which the damage was discovered. Failure to comply with the above deadline will constitute an absolute bar to the pursuit of such a claim against the Society.

Article 6

6.1. These General Conditions shall be governed by and construed in accordance with United Arab Emirates (UAE) law, and any dispute arising from or in connection with the Rules or with the Services of the Society, including any issues concerning responsibility, liability or limitations of liability of the Society, shall be determined in accordance with UAE law. The courts of the Dubai International Financial Centre (DIFC) shall have exclusive jurisdiction in relation to any claim or dispute which may arise out of or in connection with the Rules or with the Services of the Society.

6.2. However,

(i) In cases where neither the claim nor any counterclaim exceeds the sum of AED300,000 (Arab Emirates Dirhams Three Hundred Thousand) the dispute shall be referred to the jurisdiction of the DIFC Small Claims Tribunal; and

(ii) for disputes concerning non-payment of the fees and/or expenses due to the Society for services, the Society shall have the

right to submit any claim to the jurisdiction of the Courts of the place where the registered or operating office of the Interested Party or of the applicant who requested the Service is located.

In the case of actions taken against the Society by a third party before a public Court, the Society shall also have the right to summon the Interested Party or the subject who requested the Service before that Court, in order to be relieved and held harmless according to art. 3.5 above.

Article 7

7.1. All plans, specifications, documents and information provided by, issued by, or made known to the Society, in connection with the performance of its Services, will be treated as confidential and will not be made available to any other party other than the Owner without authorisation of the Interested Party, except as provided for or required by any applicable international, European or domestic legislation, Charter or other IACS resolutions, or order from a competent authority. Information about the status and validity of class and statutory certificates, including transfers, changes, suspensions, withdrawals of class, recommendations/conditions of class, operating conditions or restrictions issued against classed ships and other related information, as may be required, may be published on the website or released by other means, without the prior consent of the Interested Party.

Information about the status and validity of other certificates and statements may also be published on the website or released by other means, without the prior consent of the Interested Party.

7.2. Notwithstanding the general duty of confidentiality owed by the Society to its clients in clause 7.1 above, the Society's clients hereby accept that the Society may participate in the IACS Early Warning System which requires each Classification Society to provide other involved Classification Societies with relevant technical information on serious hull structural and engineering systems failures, as defined in the IACS Early Warning System (but not including any drawings relating to the ship which may be the specific property of another party), to enable such useful information to be shared and used to facilitate the proper working of the IACS Early Warning System. The Society will provide its clients with written details of such information sent to the involved Classification Societies.

7.3. In the event of transfer of class, addition of a second class or withdrawal from a double/dual class, the Interested Party undertakes to provide or to permit the Society to provide the other Classification Society with all building plans and drawings, certificates, documents and information relevant to the classed unit, including its history file, as the other Classification Society may require for the purpose of classification in compliance with the applicable legislation and relative IACS Procedure. It is the Owner's duty to ensure that, whenever required, the consent of the builder is obtained with regard to the provision of plans and drawings to the new Society, either by way of appropriate stipulation in the building contract or by other agreement.

In the event that the ownership of the ship, product or system subject to certification is transferred to a new subject, the latter shall have the right to access all pertinent drawings, specifications, documents or information issued by the Society or which has come to the knowledge of the Society while carrying out its Services, even if related to a period prior to transfer of ownership.

Article 8

8.1. Should any part of these General Conditions be declared invalid, this will not affect the validity of the remaining provisions.

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.

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.

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.