Guide for Shipyards to assign new buildings with CS-Ready additional class notation

Effective from 1 June 2024

www.tasneefmaritime.ae

+971 2 6922333 +971 2 4454333 info@tasneef.ae 111155, Abu Dhabi, UAE

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

INDEX

Section 1 - INTRODUCTION

1. GENERAL

The additional class notation **CS-Ready (Cyber Resilience Ready)** is assigned, according to Pt A, Ch 1, Sec 2, [6.14.71] of Tasneef Rules for the Classification of Ships, to a ship whose Shipbuilder Integrator (SBI) complies with the requirements in this Guide. These requirements are applied by the Society when performing cybersecurity reviews and surveys of operational technology (OT) control systems and related information technology (IT) systems on ships and offshore units.

1.1 System specific requirements

a) The additional class notation CS-Ready requires the application and documentation of cybersecurity protections and procedures during the manufacture of cyber-enabled products by Original Equipment Manufacturer (OEMs), and during ship construction of cyber-ready ships by SBI.
b) This Guide presents an approach to verify implemented technical cybersecurity protective mechanisms and controls that are supported by organizational management system processes and business rules (i.e., controls). Verifications are performed by reviewing pertinent documentation and performing onboard surveys.
c) Throughout this Guide, requirements are described on two levels:
   - System Specific
   - Shipbuilder Integrator (SBI) - Specific
d) Even if System Specific requirements are not a prerequisite for the additional class notation **CS-Ready** implementation, however the documentation required at System Specific level significantly supports the implementation of **CS-Ready** notation requirements.
e) The System Specific requirements indicate that the OEM has developed, embedded, and described cybersecurity capabilities for the system in scope and that the OEM has communicated existing potential cybersecurity vulnerabilities to the SBI and owner/operator for the purposes of onboard system integration and additional Cyber Risk Management implementations, as and when applicable.
f) The systems in scope of this notation are systems for Primary and Secondary Essential Services and supplementary OT or IT systems or functions connected to Primary Essential Services systems.

2. APPLICATION AND SCOPE

2.1 Application

This Guide is intended for use by organizations operating all types of ships and offshore units contracted for construction before 1st July 2024. For ships and offshore units contracted for construction on or after 1st July 2024, Pt C, Ch 3, Sec 4 of Tasneef Rules for the Classification of Ships apply.
This Guide is not intended to address every possible security contingency, but rather provide a means by which the provider/builder/operator may execute a security program that can reveal the need for unique security controls during ship operation.

2.2 Classification Scope

Compliance with the requirements in this Guide may result in **CS-Ready** notation for a Society classed ship with cyber-enabled functions. The scope is limited to Primary and Secondary Essential Services and supplementary OT or IT systems or functions digitally connected to Primary Essential Services systems.
Primary Essential Services are those services considered necessary for continuous operation to maintain propulsion and steering as well as services that are essential for safety in an emergency.
Definitions of Primary and Secondary Essential Services are described in Pt C, Ch 2, Sec 1 of Tasneef Rules for the Classification of Ships. For examples of Primary Essential Services, refer to Tab 1. This activity may also include supplementary integrated OT control and related IT systems that potentially impact automated systems integrity and security. Composite or integrated functions such as propulsion management systems will be reviewed as priority combinations of Primary Essential Services.
Non-safety-related connected control systems or information systems, and non-safety-related supplementary connected equipment are not included in the notation. However, if a review of the ship's Primary Essential Services and connected system architecture determines that the verification plan omits cyber-enabled equipment deemed important by the Society, that equipment may be added to the verification plan for the notation assessment.

Section 1 - INTRODUCTION

Table 1: Primary / Secondary Essential Services
(Services may be added or omitted depending on the OT architecture of the specific ship)

	Primary essential services *(Primary essential services are those which need to be in continuous operation to maintain propulsion and steering)*
a)	Steering gear
b)	Pumps for controllable pitch propellers
c)	Scavenging air blowers, fuel oil supply pumps, fuel valve cooling pumps, lubricating oil pumps and cooling water pumps for main and auxiliary engines and turbines necessary for the propulsion
d)	Forced draught fans, feed water pumps, water circulating pumps, condensate pumps, oil burning installations, for steam plants or steam turbines ship, and also for auxiliary boilers on ship where steam is used for equipment supplying primary essential services
e)	Azimuth thrusters which are the sole means for propulsion/steering with lubricating oil pumps, cooling water pumps
f)	Electrical equipment for electric propulsion plant with lubricating oil pumps and cooling water pumps
g)	Electric generators and associated power sources supplying the above equipment
h)	Hydraulic pumps supplying the above equipment
i)	Viscosity control equipment for heavy fuel oil
j)	Control, monitoring and safety devices/systems for equipment for primary essential services
k)	Speed regulators dependent on electrical energy for main or auxiliary engines necessary for propulsion
l)	The main lighting system for those parts of the ship normally accessible to and used by personnel and passengers
	Secondary essential services *(Secondary essential services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the ship's safety)*
a)	Windlasses
b)	Fuel oil transfer pumps and fuel oil treatment equipment
c)	Lubrication oil transfer pumps and lubrication oil treatment equipment
d)	Preheaters for heavy fuel oil
e)	Sea water pumps
f)	Starting air and control air compressors
g)	Bilge, ballast and heeling pumps
h)	Fire pumps and other fire-extinguishing medium pumps
i)	Ventilation fans for engine and boiler rooms
j)	Services considered necessary to maintain dangerous cargo in a safe condition
k)	Navigation lights, aids and signals
l)	Internal safety communication equipment
m)	Fire detection and alarm systems
n)	Electrical equipment for watertight closing appliances
o)	Electric generators and associated power supplying the above equipment
p)	Hydraulic pumps supplying the above equipment
q)	Control, monitoring and safety for cargo containment systems
r)	Control, monitoring and safety devices/systems for equipment for secondary essential services

Section 1 - INTRODUCTION

3. NOTATION

The additional class notation **CS-Ready** will be assigned upon demonstrating compliance with the requirements given in this document. The applicability and purpose of this notation is indicated in Tab 2.

Table 2

Notation	Applicable to	Purpose
CS-Ready	A specified ship whose Shipbuilder Integrator (SBI) complying with the requirements in this Guide	Notation documents that cybersecurity procedures and protections are applied to critical OT/IT systems during ship construction and are documented and communicated to the Owner per Section 2. This notation provides OT/IT system information that can be utilized to satisfy certain requirements described in Pt C, Ch 3, Sec 5 of Tasneef Rules for the Classification of Ships

Computer-based control systems within the scope of the additional class notation **CS-Ready** will be listed in the OT/IT Digital Architecture Description to describe the exact coverage of the applicable notation. For example, the scope could be limited to one or more of control systems such as:

- Propulsion and Steering Control Systems
- Navigation Control Systems
- Power Management Control System
- Drilling Control System

4. DEFINITIONS AND ABBREVIATIONS

4.1 Definitions

4.1.1 Company

The Company is the Owner of the ship, or any organization or entity that operates the ship and has agreed to assume roles and responsibilities imposed by the ISM Code and this Guide. The Company can also be the organization that owns the operational technology and connected information systems aboard the ship and initiates a security program or project for the ship.

4.1.2 Shipbuilder Integrator (SBI)

For a ship under major modification or construction as a newbuild, the SBI is the shipyard. The shipyard may utilize subcontractor integration services or provide those services in-house. If the SBI provides in-house integration services, it is expected to provide developed technical and operational system integration information to the Company. If the SBI utilizes a third-party for system integration services, the SBI is expected to aggregate and provide subcontractor-developed technical and operational system integration information to the Company upon delivery of the ship.

4.1.3 Service Supplier (SS)

Service Supplier (SS): A person or company, not employed by an IACS Member, who at the request of an equipment manufacturer, shipyard, vessel's owner or other client acts in connection with inspection work and provides services for a ship or a mobile offshore unit such as measurements, tests or maintenance of safety systems and equipment, the results of which are used by surveyors in making decisions affecting classification or statutory certification and services.

4.1.4 Sub-Supplier (Sub-System or Component Providers)

A Sub-Supplier is a provider of equipment parts or subcomponents embedded in or connected to SS equipment systems and is included in integration testing and verification.

4.1.5 Other definitions

The definitions listed below have been taken or adapted from various sources including the ISM Code, ISO 9000:2015, ISO 14001:2015, ISO 50001:2018, ISO 45001:2018 and CNSSI 4009.

a) Boundary. Physical or site limits, organizational limits, system architecture limits, and/or logical limits around IT or OT systems or functions as defined by the Company.
b) Capability. The ability to execute a specified course of action.
c) Company. See Sec 1, [5.1] in this Guide.

d) Complex Connection. A digital communications path between equipment and a network that supports other digital communications but is not connected to the Internet.
e) Control System. Set of devices that manages, commands, directs, or regulates the behavior of other devices, equipment, or equipment systems according to user inputs, settings, or configurations.
f) Critical Function. A systemic role, usually performed by Primary Essential Services or the equivalent, upon which unit, system, or Company mission, business process, safety task or security purpose depends to the extent that failure of the systemic role causes failure of the mission, process, task or purpose.
g) Cyber-Enabled System. Computerized or programmable system built to provide significant degrees of automation in operational function, system monitoring and management, or data communications.
h) Cyber Event. A detected cyber-related anomaly in a cyber-enabled system.
i) Cyber Hygiene. Best practices implemented within cybersecurity programs that improve cybersecurity while performing administrative and operational activities, including but not limited to e-mailing, web searching, and text messaging.
j) Cyber Incident. A cyber event that results in the corruption of data or the interruption of service in a cyber-enabled system.
k) Cyber Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (US, Committee on National Security Systems Glossary, NSSI 4009,2010)
l) Cybersecurity. Activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and defended against damage, unauthorized use or modification, or exploitation.
m) Cybersecurity Representative. A chartered organizational entity or person responsible for implementation and maintenance of a cybersecurity risk management program and/or system(s). The ashore person in charge of this office may be referred to as the Chief Information Officer (CIO), Cyber Security Representative or Cybersecurity Designated Person Ashore (DPA). The onboard person responsible for cybersecurity may be referred to as the Electro-Technical Officer (ETO) or the Chief Engineer.
n) Cybersecurity Risk Assessment. Overall process of evaluating the risk(s) arising from cybersecurity-related characteristics that may affect the control, availability, integrity, or confidentiality of systems and their functions. The assessment takes into account the adequacy of any existing controls, and the acceptability of the risk to the organization based on anticipated consequences of failure to the Company.
o) Cybersecurity Risk Management System (CRMS). An organizational system that provides technological and procedural cybersecurity protections.
p) Discrete Connection. A digital communications path characterized by one direct connection (not networked) to one piece of equipment, but not to the Internet.
q) Documentation. Descriptions, graphical representations, records, and certificates that confirm that the ship is in compliance with applicable cybersecurity and/or Cyber resilience security requirements.
r) Essential Services (Primary and Secondary). Services considered necessary for continuous operation to maintain propulsion and steering (primary essential services), non-continuous operation to maintain propulsion and steering and a minimum level of safety for the ship's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services), and emergency services as described in Pt C, Ch 2, Sec 1 of Tasneef Rules for the Classification of Ships.
s) Federated Systems. Systems that work together in an interoperable way that allows data sharing, where each system has separate functionality.
t) Functional Description Document (FDD). Revision-controlled document containing a description of the industrial control system (ICS) equipment, control systems, and data flows in a form readily understandable by shipboard personnel who are technically competent in shipboard operations, and authorized to evaluate, operate, or maintain those equipment and control systems.
u) Hazard. Source, situation, or act with a potential for harm, in terms of injury or ill health, damage to property, damage to workplace environment, or a combination of these.
v) Industrial Control System (ICS). Computer-based control system for industrial or machinery processes.
w) Industry Working Group Guidelines (IWGG). Documented Guidelines on Cyber Security Onboard Ships, Volume 3, produced by an industry working group comprised of BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and World Shipping Council.
x) Information System. Automated system that enables Company and business process use of data.
y) Information Technology. Automated systems used for storing, retrieving, processing, and sending data.

z) Infrastructure. System of facilities, equipment, and services needed for the operation of the Company.
aa) ISM. International Management Code for the Safe Operation of Ships and for Pollution Prevention. Also referred to as the International Safety Management Code.
bb) NIST Cyber Security Framework Core Functions or Elements: Identify, Protect, Detect, Respond, Recover.
cc) Objective. An achievable goal set by the Company stated in terms of the management system's performance.
dd) Operational Technology. Automated systems, including hardware and software, that perform direct monitoring and/or control of physical devices, processes, or events. It is a superset of industrial control systems that includes monitoring, sensing, and human interface devices, as applicable to an installation.
ee) Qualitative Risk Assessment. Risk review method that relies on experience and expert opinions to assign likelihood of incident occurrence graded as unlikely-to-likely, and relative impact of incident occurrence graded as low-to-high.
ff) Quantitative Risk Assessment. Risk review method that relies on identified cybersecurity risk contribution elements as represented by maritime and offshore personnel, software, digital devices, and digital architectures, and assigns numeric values to the relative likelihood that those elements will contribute to a mission or safety critical incident.
gg) Remote Access. A method of gaining access to distant ships through network digital connections. This may refer to personnel access to network resources, such as through Virtual Private Network (VPN), or it may refer instead to direct connection to control systems equipment by connection utilities (i.e., secure shell).
hh) Risk Assessment. Overall process of evaluating the risk(s) arising from an identified risk contributor, taking into account risk tolerance and the adequacy of any existing controls.
ii) Safety-Critical System. A cyber-enabled component or system installed in a ship, facility, or mission system that is necessary to carry out critical functions, and which, through failure or incomplete operation, may cause safety impacts to personnel, to the ship or to the environment.
jj) Safety Management System (SMS). A structured and documented system enabling Company personnel to effectively implement the Company safety and environmental protection policy. In the Cyber Resilience context, the SMS is complementary to the Cybersecurity Risk Management System for cross-domain safety of cyber-enabled systems. SMS is required as an active management system under the ISM Code.
kk) Service Supplier (SS). An organization that may hold a system Type Approval or other recognition offered by the Society for qualified suppliers who offer specialized services and enhance existing marine and offshore safety practices. (Ref "Tasneef Rules for the certification of service suppliers", Annex 1)
ll) Simple Connection. A direct digital communications path between one piece of equipment and one or more other pieces of equipment (not networked), but not to the Internet.
mm) SOLAS Convention. The International Convention for Safety of Life at Sea, 1974, as amended.
nn) Very Large Network Connection. A direct digital communication path between cyber-enabled equipment or network(s) to a node or endpoint accessible to a very large number of digital identities, such as the Internet.
oo) Vulnerability. Used here, a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-53. It is a weakness that allows a digital device, endpoint, or software application to be accessed by an unauthorized digital or human identity and digitally corrupts or affects the functionality of the system or network.

4.2 Abbreviations

CRMS Cybersecurity Risk Management System
FDD Functional Description Document
FMEA Failure Mode and Effects Analysis
ISM International Safety Management Code
IT Information Technology
IWGG International Working Group Guidance
MOC Management of Change
MSC Maritime Safety Committee
NIST National Institute of Standards and Technology
OCIMF Oil Companies International Marine Forum
OEM Original Equipment Manufacturer

Section 1 - INTRODUCTION

OT Operational Technology
RO Recognized Organization
SBI Ship Builder Integrator
SIEM Security Information Event Management
SIM Security Information Management
SEM Security Event Management
SMS Safety Management System
SS Service Supplier
TMSA3 Tanker Management and Self-Assessment Best Practice Guide, Third Ed

5. Process

5.1 General

To obtain the additional class notation **CS-Ready** an engineering review of documentation is required, followed by an implementation survey on board the ship.

System Specific requirements and Certification (ie. Type Approval), in accordance with Pt C, Ch 3, Sec 5 of Tasneef Rules for the Classification of Ships, is granted to a specific cyber-enabled system that is installed on board and encourages a full lifecycle collaboration between the system provider and the owner/ operator concerning cybersecurity. In addition, recognizes a specific system installation as having been built in a cyber-secure environment, assessed for cyber risk during design and construction, and installed with documented cyber risk management recommendations or embedded protections.

System Specific Certification calls for documented communication of cybersecurity information to the shipbuilder/integrator and owner/operator so that they understand their responsibilities for applying disciplined onboard cybersecurity practices to maintain the integrity of embedded security protections for the installed life of the system.

While System Specific requirements are responsibility of the system provider, the shipbuilder, system integrator, and owner/operator inherit some or all of the responsibility for maintaining the cybersecurity integrity of the installed system throughout its lifecycle as provided:

a) in this Notation
b) in Pt C, Ch 3, Sec 4 of Tasneef Rules for the Classification of Ships and
c) in supply chain business arrangements.

The additional class notation **CS-Ready** provides a foundation for compliance with Cyber Resilience requirements described in Pt C, Ch 3, Sec 4 and Sec 5 of Tasneef Rules for the Classification of Ships, by requiring the SBI to collect and compile information provided by system providers and communicate both cybersecurity design and implementation information to the ship owner or manager (Company). This information is made available to the Company to expedite the process of collecting information required for compliance. To gain the most benefit from the **CS-Ready** notation, the Company may apply for Ship Cyber Resilience Certification in compliance with Pt C, Ch 3, Sec 4 and Sec 5 of Tasneef Rules for the Classification of Ships prior to expiration of the additional class notation **CS-Ready**, which occurs at the first annual inspection of the ship.

5.2 Cyber Safety Reviews

Cyber Safety engineering reviews for **CS-Ready**, or Ship Cyber Resilience Certification in compliance with Pt C, Ch 3, Sec 4 and Sec 5 of Tasneef Rules for the Classification of Ships, are initiated by the client and follow a uniform process that includes a survey of the implementation on board a ship.

5.3 Conditions

The given notation is a representation by the Society that, at the time of survey, cybersecurity processes and protections have been implemented in accordance with the requirements in this guide, as well as satisfactory completion of assessments, inspections, tests, and audits. Management of the performance of surveyed systems remains the responsibility of the Company.

5.4 Termination

The maintenance of certification or this additional class notation is conditional upon the continued compliance of the Company and the ship with the requirements of this Guide. Failure by the Company or the ship to continue to comply results in termination of related certification and/or notation.

If shipowner or management of the ship changes, the Society reserves the right to request an additional engineering review and/or implementation survey to confirm that the notation remains valid.

6. PLANS AND DATA TO BE SUBMITTED

The additional class notation **CS-Ready**, Plans and Data to be Submitted, consist of:
a) System Specific and
b) SBI - Specific. Even if System Specific requirements are optional for the additional class notation **CS-Ready** implementation, however documentation required at System Specific level significantly supports the implementation of additional class notation **CS-Ready** requirements.
The Society review and verify documents and implementation that are key to this Notation and relevant to Cyber Resilience certifications as per Pt C, Ch 3, Sec 4 and Sec 5 of Tasneef Rules for the Classification of Ships. Documentation describing these implementation categories is reviewed by the Society prior to an onboard verification survey. This practical approach promotes the completeness of a Company cybersecurity program and supports a comprehensive and efficient the Society assessment.
While the breadth of successful maritime cybersecurity programs is consistent across eight basic program activities, the depth of those activities is scalable based on the relative digital complexity of critical cyber-enabled systems on board Company ships, and the cyber-related risks presented by the design, connectivity, and operation of those systems.
The requirements for the notation are referenced in Section 2.
The documentation to be provided for the Society Engineering review listed in this section, is detailed in Sec 2, and is organized into eight fundamental cybersecurity documents and implementation categories summarized as follows:

1) Cybersecurity Representative(s) or Organization. Internal or third-party representative(s) responsible for implementation of a Company-wide cybersecurity program, with supporting documentation indicating authorities, responsibilities, and organizational position.
2) Cybersecurity Policies and Procedures. Policies and procedures that document Company cybersecurity governance and guidance for employees and third parties (e.g., suppliers, contractors, guests).
3) Incident Response and Recovery Team. Internal and/or third-party (i.e., a person or team) responsible for Company response to a cybersecurity incident, including documented levels of authority, team responsibilities, and lines of communication between and among shore and shipboard personnel.
4) OT/IT Digital Architecture Description. A technical description of a cyber-enabled functional system or system-of-systems that is suitable for performing a cybersecurity risk assessment and includes primary function(s), digital connections, data flows, and digital endpoints.
5) Risk Assessment and Management Plan. A documented risk assessment that identifies cybersecurity risk contributors present in essential cyber-related OT systems and connected IT systems, and a documented plan establishing appropriate safeguards for resolving identified risk contributors with specific risk mitigation business choices, technological solutions, and procedures.
6) CRMS Design and Implementation Procedures. A documented description of technical and procedural cybersecurity controls specified based on risk management requirements contained in a risk management plan.
7) Cybersecurity Training Program. A documented training program based on cybersecurity training requirements that is implemented for internal and third-party personnel (as appropriate) whose responsibilities and authorities may affect essential cyber-enabled OT systems.
8) Management of Change (MOC) Procedures. A documented software, computer hardware, and equipment change management procedure applied to control and record essential cyber-related OT control system changes.

Three of the eight documents and implementation activities pertain to each ship (items 4, 5, and 6 above), but are supported by the remaining five enterprise-wide documents and activities (items 1, 2, 3, 7, and 8). Risk assessment and management (item 5) defines the scale or depth of technical and procedural content of a cybersecurity program. This approach provides a framework for building and sustaining a security program based on observed risk assignable to specific ships and individual Company objectives.
This approach also provides for and encourages the application of security controls and requirements selected by the company from other sources, such as NIST's Cybersecurity Framework; the ISO 27000 (series); international requirements from MSC-FAL.1/Circ.3; and from industry working group guidelines, such as the International Working Group Guidelines on Cyber Security Onboard Ships v3 (IWGG) or the OCIMF Tanker Management and Self-Assessment Best Practice Guide, Third Ed. (TMSA3).
The documentation required for the **CS-Ready** notation is summarized in the following paragraphs. [6.1] is optional for **CS-Ready** notation, however documentation required at System Specific level significantly supports **CS-Ready** notation requirements.

6.1 System Specific - Documentation to be submitted

6.1.1 System OT/IT Architecture
Documentation describing the product system architecture.

6.1.2 Risk Assessment and Management Plan
Documentation detailing a product vulnerability analysis, including a report detailing an internal review of cybersecurity risk inherent to OEM product(s) and risk mitigation methods implemented or recommended.

6.1.3 Installed CRMS Design and Implementation
Documentation describing cybersecurity protective functions embedded in the product, including anti-malware scanning procedures.

6.2 SBI Specific - Documentation to be submitted
The documentation required in order to receive the CS-Ready notation, listed below is organized based on the previously described documentation categories.

6.2.1 SBI Cybersecurity Representative or Organization
SBI to provide documentation identifying person(s) responsible for cybersecurity, the organizational position within the SBI, and quality or cybersecurity certificates (e.g., ISO/IEC 27001, ISA/IEC 62443, or other related certifications).

6.2.2 SBI Cybersecurity Policies and Procedures
SBI to provide documentation detailing cybersecurity policies and implementation procedures applied to employees, suppliers, and contractors.

6.2.3 Company and Ship OT/IT Digital Architecture Description
Functional descriptions and diagrams detailing the digital connections and boundaries of cyber- enabled OT systems and digitally connected IT systems installed on the ship.

6.2.4 Company and Ship CRMS Design and Implementation Procedures
CRMS functional description document (FDD) detailing the cybersecurity equipment inventory aboard the ship, a graphical description of that system architecture, and included logical and procedural protections.

6.2.5 SBI Management of Change (MOC) Procedures
Documentation detailing change management and configuration control policies and procedures applied during ship construction, including OT, OT-connected IT, and CRMS software and computer hardware registries.

Section 2 – NOTATION REQUIREMENTS

1. CS-READY NOTATION REQUIREMENTS

CS-Ready notation requirements consist of:

a) System -Specific and

b) SBI - Specific Requirements.

Ref also to [7].

System Specific - Certification (ie. Type Approvals) in accordance with Pt C, Ch 3, Sec 5 of Tasneef Rules for the Classification of Ships and **CS-Ready** notation are complementary and provide detailed supply chain assessment of Cyber resilience for the lifecycle of the ship. This approach acknowledges the shared responsibilities of supply chain participants and places those responsibilities with the people who are best positioned to implement and sustain cybersecurity solutions. It also indicates that the OEM has communicated existing potential cybersecurity vulnerabilities to the Shipbuilder/Integrator (SBI) and owner/ operator for the purposes of onboard system integration with other onboard systems and additional CRMS implementations, if applicable.

1.1 System Specific - Requirements (optional)

i) OEM is to define and document the digital boundary of the computer-based system.

ii) OEM is to document the computer-based system as being installed on an identified ship, and:

a) Performing Primary Essential Services; or,

b) Encompassing at least one subsystem within the OEM System's defined Primary Essential Services digital boundary; or,

c) OEM system is to be digitally connected (i.e., wired or wireless connection) to a system or subsystem outside of the OEM System's defined digital boundary that performs Primary Essential Services. The hardware equipment on which the OEM software executes is to be approved by the Society (i.e., Design Assessed or Type Approved).

iii) The OEM system may have an active Type Approval Certificate (if applicable).

iv) OEM is to deliver system documentation in accordance with this Guide and Pt C, Ch 3, Sec 5 of Tasneef Rules for the Classification of Ships to the shipbuilder during construction. The shipbuilder is to maintain system documentation during construction and provide system documentation to the owner/operator upon ship commissioning, in accordance with Pt C, Ch 3, Sec 4 of Tasneef Rules for the Classification of Ships. The owner/operator is to maintain the installed system and system documentation during operation in accordance with system provider maintenance agreements and the above-mentioned the Tasneef Rules for the Classification of Ships.

Table 1: System Specific – Requirements (optional)

	System Requirements	**References**
1.	System identifying characteristics are documented, and include the following content: • Computer-based system or subsystem description, unique model number, name, serial number(s) or equipment tracking identifier. • System software application version number(s) at the time of Factory Acceptance Test of the initial system. • System firmware version number(s) for computer-based components implemented at Factory Acceptance Test (FAT) of the initial system.	Sec 1, [6], 4) OT/IT Architecture
2.	System digital connectivity characteristics are documented, and include the following content: • Characterization of the digital connection complexity of the system as Discrete, Simple, Complex, or Very Large Network. • Wireless connection access points and configurations (Wi-Fi, cellular-based broadband, Bluetooth, RF datalink, etc.). • System-wide time source for computer-based systems or the capability to timestamp security events for components. • List of enabled or disabled digital services and ports (Ports, Protocols and Services (PPS)). If PPS are project dependent, state, "PPS are project dependent."	
3.	System connection architecture topology diagram documents: • Digitally enabled subsystems, components, and network infrastructure components. Remote Input and Output (I/O) connections may be shown as a single connection regardless of the number of I/O connections;	

	• HMIs and control panels connected to OT network(s); • Sub-supplier's and contracted and known third-party control and IT equipment connected to OEM's OT network(s); • IT network connection(s) to the OEM system or system network(s); and, • Data collection connection(s). • Satellite remote access connection(s). • Wireless connection point(s).	
4.	Internal risk assessment of the OEM product(s) is performed and documents: • OT function(s) performed by the system; • Overall Integrity Level (IL) – (as per IEC 61508-5 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5). Examples of methods for the determination of safety integrity levels designation as assigned by the OEM, including a description of OT functionality in normal, degraded, and failed states; • Safety FMEA report, if required by other Tasneef the Rules for the Classification of Ships or Guides (If none required, the OEM is to state, "No FMEA required by Tasneef the Rules for the Classification of Ships Guides"); • Controlled Equipment List; • Assessment of risk contributors classified in OEM Vulnerability Table; • Unremediated risks and recommended cybersecurity protective functions (hardware or software); and, • Potential vulnerabilities associated with any wireless networks and remote connections.	Sec 1, [6], 5) Risk Assessment and Plan
5.	Third-party risk control methods or technologies recommended by the OEM but not installed are documented and identified as being either OEM-tested or not tested.	
6.	Cybersecurity technologies or procedures for network protection implemented by the OEM or OEM sub-supplier are documented.	Sec 1, [6], 6) CRMS Design
7.	OEM anti-malware scans performed during final acceptance test for the computer-based system are documented and include name of the ship on which the scanned system will be installed, scan date, scan results, and anti-malware software name/version number.	
8.	OEM documents cybersecurity measures applied during remote digital connection to the fielded computer-based system concerning: • OEM cybersecurity policy governance applied to remote connection to ships. • Method used for remote session termination (e.g., automatic time-out or specified time-out criteria). • Number of remote concurrent sessions allowed, controls or limitations. • Classifications of data authorized for remote transfer. • Use of encrypted channels or applications required to protect remote transfer. • Identity management controls applied to personnel authorized to access client ships.	
9.	Description of security procedures or monitoring tools (e.g., SEM, SIM, SIEM applications) employed by or recommended for managing unauthorized access to this computer-based system or component are documented.	
10.	Descriptions of process used for performance data and system logs collection and analysis are documented.	
11.	Descriptions of intrusion detection or intrusion protection system built into the computer-based system or component are documented.	
12.	Descriptions of number of allowed local concurrent sessions and how sessions are limited or controlled and terminated are documented.	
13.	Descriptions of undocumented, developer-specific, or backdoor access accounts removed before delivery are documented.	
14.	Descriptions of known vulnerabilities associated with web server, if enabled, are documented.	
15.	Descriptions of implemented security controls associated with wireless networks and remote connections are documented.	

1.2 SBI Specific - Requirements

The **CS-Ready** notation is applicable to the Shipbuilder/Integrator (SBI). It establishes requirements for maintaining the integrity of cyber-enabled systems during ship construction, system integration, and product

delivery. During ship construction and integration, the requirements for the **CS-Ready** notation guide Shipbuilders to reference and apply Service Supplier cybersecurity documentation, configurations, drawings and interface information as described in the System Specific – Requirements and/or related System/s Certification.

The **CS-Ready** notation, Service Supplier requirements also enable the Shipbuilder to subsequently transfer applicable cybersecurity technical and procedural information to the Company to support any post-delivery addition of cybersecurity capabilities. System/s Specific requirements are optional for **CS-Ready** notation implementation, however documentation required at System/s Specific level significantly supports **CS-Ready** notation requirements.

Table 2: SBI Requirements

	SBI Requirements	**References**
1.	Identity or identities of the person or persons responsible for cybersecurity during the construction of the ship are documented and provided to the Company on delivery of the ship.	ISM Code MSC-FAL.1 /Circ.3, 1.3 NIST CSF: All IWGG Annex 2 1 – CS Representative
2.	Copies of any quality certifications held by the SBI documented and provided to the Society.	
3.	Cybersecurity policies and procedures applied to installed systems, workstations, and devices during construction are documented by the SBI and provided to the Company upon delivery of the ship.	ISM Code MSC-FAL.1 /Circ.3, 1.5 NIST CSF: Identify, Protect IWGG Annex 2 2 – Policies and Procedures
4.	Functional Description Documents (FDDs) of individual systems installed on the ship are compiled by the SBI for delivery to the Owner/Operator. The SBI develops a comprehensive FDD of the integrated OT/IT system installed on the ship. SBI provides the FDD to the Owner/Operator upon ship delivery. The comprehensive FDD describes: • Network diagram(s) indicating system physical and digital boundaries. • System IP addresses of networked or serial communications, ports, protocols, and services (PPS) enabled or disabled for normal operations (PPS may be separately listed with references to the diagram). • System connections enabled for remote monitoring or maintenance (remote I/O modules are to be shown as a single line regardless of the • number of remote digital connections and locations). • Cybersecurity protections embedded in or installed by the OEM to protect the system.	ISM Code MSC-FAL.1 /Circ.3, 2.1.2 NIST CSF: Identify IWGG Annex 2 4 – OT/IT Architecture
5.	The SBI develops a comprehensive FDD describing the cybersecurity risk management system (CRMS) installed to protect the integrated OT/IT system installed on the ship. SBI provides the FDD to the Owner/Operator upon ship delivery. The comprehensive CRMS FDD describes: • CRMS technological and procedural functions (i.e., hardware and associated hardware) applied to installed systems, workstations, devices, and digital endpoints during construction. • Descriptions of access protections such as procedures, keys, and passwords applied during construction, including information or devices needed to decommission physical and logical blocking methods. • Virus detection/removal software version numbers used during OEM system final acceptance testing prior to delivery are to be included in the ship CRMS FDD.	ISM Code MSC-FAL.1 /Circ.3, Multiple NIST CSF: Protect, Detect IWGG Annex 2 6 – CRMS Design
6.	Ship OT and connected IT equipment and supporting software are to be maintained under revision control during ship construction and change management records of system updates are to be provided by the SBI to the Owner/Operator upon delivery of the ship.	ISM Code MSC-FAL.1 /Circ.3, 2.1.8 NIST CSF: All IWGG Annex 2 8 – Management of Change
7.	Functional Description Document (FDD) of the ship OT and connected IT systems are to be maintained under revision control during ship construction and provided by the SBI to the Owner/Operator upon delivery of the ship.	
8.	Ship CRMS hardware and software are to be maintained under revision control during ship construction and change management records of system updates are to be provided by the SBI to the Owner/Operator upon delivery of the ship.	
9.	Functional Description Document (FDD) of the ship CRMS is to be maintained under revision control during ship construction and provided by the SBI to the Owner/Operator by the SBI upon delivery of the ship.	

Section 3 – SURVEYS

1. GENERAL

This Section outlines the Class survey requirements for Ships under construction which are eligible for the **CS-Ready** notation. The scope of survey will include the critical systems (primary and secondary essential services) defined and agreed between the SBI and the Society based on the description and documentation provided by the SBI.

CS-Ready Survey requirements consist of: a) System/s - Specific and b) SBI Specific, Survey requirements. System/s Specific requirements are optional for **CS-Ready** notation implementation, however documentation required at System/s Specific level significantly supports **CS-Ready** notation requirements.

2. SURVEYS DURING CONSTRUCTION

2.1 System Specific - Initial Surveys (optional)

The Surveyor is to verify the following documentation to be provided by the SBI, OEM's, or the service supplier are maintained by the owner/operator onboard the ship for the system named in an active CS-System notation.

i) Contact information of person or persons responsible for system provider enterprise and product cybersecurity is documented and maintained aboard the ship.

ii) Service supplier cybersecurity policies and procedures governing system provider employee access to fielded systems are documented and maintained aboard the ship.

iii) Service supplier cybersecurity incident response team capabilities and contact information is documented and maintained aboard the ship.

iv) Service supplier documentation uniquely identifies the system and describes digital boundaries and connectivity characteristics in a system connection topology diagram.

v) Service supplier documentation details the results of a system cybersecurity risk assessment performed by the system provider.

vi) Service supplier documentation details risk control procedures or technologies embedded in the system. Risk control methods recommended by the system provider are documented and identified as being installed or not installed.

vii) Service supplier documentation details cybersecurity training required for its employees concerning cyber-hygiene and security of digital devices used for accessing the installed system.

viii) Service supplier documentation details change control management procedures applied by the system provider to system software back-ups, backup storage, installation of product hardware and software updates, changes, and configurations. Surveyor may request to be informed of the location of back-up software at the survey.

2.2 SBI Specific - Initial Surveys

The Surveyor is to verify SBI physical security and change management policies and procedures applied during ship construction and refitting activities during the initial survey. Surveyor is to verify the following during construction.

i) SBI documentation defining the physical and digital boundaries of critical systems included in the scope of the **CS-Ready** notation in collaboration with OEM suppliers.

ii) SBI documentation that aggregates OEM-provided Functional Description Documents (FDD) as an integrated system FDD on board the ship.

iii) SBI document(s) that compile the inventory of cybersecurity protective equipment and technologies.

iv) SBI documentation that provides to the Company a digital architectural description diagram that includes installed computer-based system(s) and network(s).

v) SBI documentation that provides to the Company computer software and hardware registries.

vi) SBI documentation that describes access protection/control for installed equipment.

vii) SBI has blocked or disabled accessible USB and network ports. If disabled, no testing is done by the Society.

viii) SBI documentation that describes installed cybersecurity functions.

CS-Ready notation expires when the first annual inspection of the ship is performed and may not be extended or renewed.

3. SURVEYS AFTER CONSTRUCTION

For requirements for surveys after construction, the Pt C, Ch 3, Sec 4 of Tasneef Rules for the Classification of Ships apply.

Section 3 – SURVEYS

4. MODIFICATIONS

Any modifications to the original ship design or systems selection need to be officially communicated by the SBI to the Society and agreed by both parties, allowing sufficient time for the Society review / approval, surveying activities and test witnessing.

5. PARTIAL COMPLIANCE

The ship is surveyed for the degree of compliance. Upon the Company's request, the Society may report the current degree of compliance if the ship has partially implemented the Notation requirements. the Society Engineering review and approval are required prior to the Society Surveyor's attendance.