Guide for

Cybersecurity Implementation for the Marine and Offshore Industries

ABS CyberSafety® Volume 2

ABS

August 2023

GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES
AUGUST 2023

ABS CYBERSAFETY® VOLUME 2

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

Foreword *(1 August 2023)*

Maritime and offshore safety and security are closely linked. For over 150 years, ABS has promoted safe and efficient commerce at sea by developing and verifying the application of standards. Initially, the emphasis was on safety alone, and ABS focused its energies on preventing accidents caused by human error and physical failures of engineered systems. The roots of those causes are complex, but they have been managed by continuously improving analysis methods that increased industry's ability to understand and predict unsafe conditions and practices. The result of this dedication and diligence is the steady improvement of maritime and offshore safety for many years.

In the past decade, expanding automation has introduced an additional root cause of engineered system failures to the marine and offshore industries: *cyber insecurity*. These failures are directly attributable to functional faults having a number of root causes or combinations of those causes. Even so, they tend to cluster around a relatively few general causes: software flaws, network complexity, increased digital connectivity, human error, and deliberate actions taken by individuals intending to cause harm.

It is clear that increased automation and digital connectivity demand that vessels control their cyber risk. This makes cybersecurity another engineering discipline essential to maritime and offshore system reliability, safety, and security. In this context, cybersecurity refers to the security of information networks and the control systems of equipment that communicate, store, and use data onboard a vessel and throughout the connected supply chain.

In the maritime and offshore supply-chain, cybersecurity is applicable to cyber-enabled equipment systems installed in vessels, offshore assets, and ports. It includes maritime and offshore industry equipment suppliers, digital infrastructure and component parts suppliers, subcontractors, and technicians throughout the supply chain who must develop and expand cybersecurity management capabilities within each participating organization to adapt to constantly evolving cyber risks.

This document is Volume 2 of the ABS CyberSafety® series. It provides cyber-related safety and security requirements and recommendations for the assessment of Company cybersecurity systems. It also provides guidance for vessel readiness for preventing and managing cyber events that may compromise the safety and security of the data, systems, and vessels of a Company or organization. The notations presented in this Guide are offered to recognize cybersecurity protections aboard a vessel that reduce cyber risk and enhance cybersafety.

ABS offers the **CS-System**, **CS-Ready**, **CS-1**, and **CS-2** notations to vessels and offshore assets that comply with ABS requirements contained in this Guide.

For new construction vessels contracted after 1 January 2024, Section 4-9-13 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)* (IACS UR E26) is to be complied with. Any additional requirements in this Guide are optional.

The August 2023 version aligns the Guide with the latest version of the ABS *Guide for ABS CyberSafety for Equipment Manufacturers – ABS CyberSafety Volume 7*.

This Guide becomes effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of this Guide is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

CONTENTS

1 General *(1 August 2023)*

This Guide presents ABS requirements for the issuance of four (4) notations. These requirements are applied by ABS when performing cybersecurity reviews and surveys of operational technology (OT) control systems and related information technology (IT) systems on commercial vessels and offshore assets.

The four notations are:

1) **CS-System**

2) **CS-Ready**

3) **CS-1**

4) **CS-2**

The **CS-System** and **CS-Ready** notations require the application and documentation of cybersecurity protections and procedures during the manufacture of cyber-enabled products by OEMs, and during vessel construction of cyber-ready vessels by Shipbuilders/Integrators.

The **CS-1** and **CS-2** notations require owners and operators to minimize and manage risks to cyber-enabled systems by establishing a cybersecurity program that includes documented organizational and vessel-specific cybersecurity procedures and protections.

Maintenance of the **CS-System**, **CS-1**, and **CS-2** notations over the operational life of the vessel is subject to verification of continued compliance as evidenced by satisfactory completion of periodic surveys conducted on board the vessel or remotely.

This Guide presents the ABS approach to verifying 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 on-vessel surveys. Additional guidance on ABS CyberSafety® requirements and methods is available in other volumes of the ABS CyberSafety® series.

Additional criteria for the hardware and software integrity of computer-based control systems are given in other publications, such as:

- ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)*
- ABS *Rules for Building and Classing Mobile Offshore Units (MOU Rules)*
- ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*
- ABS *Guide for Software Quality Management (SQM)*

2   Application and Scope

2.1   Application *(1 August 2023)*

This Guide is intended for use by commercial organizations operating all types of vessels and offshore assets (see Note 2 below).

For new construction vessels contracted after 1 January 2024, Section 4-9-13 of the ABS Rules for Building and Classing Marine Vessels (Marine Vessel Rules) (IACS UR E26) is to be complied with. Any additional requirements in this Guide are optional.

2.2   Scope

The requirements in this Guide are applicable to standalone, federated, and integrated computer-based information technology and operational technology systems installed on a vessel.

2.2.1   Classification Scope

Compliance with the requirements in this Guide may result in issuance of a **CS-System**, **CS-Ready**, **CS-1**, or **CS-2** notation to an ABS-classed vessel with cyber-enabled functions. The scope of each notation is limited to Primary Essential Services and ancillary 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. See 4-8-1/7.3.3 of the *Marine Vessel Rules* or other applicable Rule set (see Note 1 below). For examples of Primary Essential Services, refer to 4-8-1/7.3.3 TABLE 1 of the *Marine Vessel Rules*, 4-1-1/Table 3 of the *MOU Rules*, and Section 1/Table 1 of this Guide. The assessment is also to include ancillary 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 ancillary connected equipment are not included in the notation unless detailed in the verification plan. However, if a review of the vessel's Primary Essential Services and connected system architecture determines that the verification plan omits cyber-enabled equipment deemed important by the Company, that equipment may be added to the verification plan and included in the business agreement in place for the notation assessment.

Notes:

1   The *Marine Vessel Rules* (Section 4-9-3) define relevant automated systems as, "Computer-based systems used for control, monitoring, safety, or internal communication systems". For vessels classed with the notation **ACCU** or those built after 2012, computerized control interface systems and controllers are automatically categorized Primary Essential Services. For all other vessels, inclusion of such systems and controllers in the scope of the notation depends on their relevance to safety and security or potential effects on Primary Essential Services.

2   This Guide applies to manned and self-propelled, existing and new marine vessels and offshore units (including liftboats), referred to as "vessels" in this Guide, for which the optional **CS-System**, **CS-Ready**, **CS-1**, and **CS-2** notations have been requested.

TABLE 1
Primary Essential Services

(Services may be added or omitted depending on the OT architecture of the specific vessel)

a)	Steering gears
b)	Pumps for controllable pitch propellers

c)	Scavenging air blower, fuel oil supply pumps, fuel valve cooling pumps, lubricating oil pumps and cooling water pumps for main and auxiliary engines, turbines and shafting necessary for propulsion
d)	Ventilation necessary to maintain propulsion
e)	Forced draft fans, feed water pumps, water circulating pumps, vacuum pumps and condensate pumps for steam plants on steam turbine vessels or offshore units, and also for auxiliary boilers where steam is used for equipment supplying primary essential services
f)	Oil burning installations for steam plants on steam turbine vessels or offshore units and for auxiliary boilers where steam is used for equipment supplying primary essential services
g)	Low duty gas compressor and other boil-off gas treatment facilities supporting boil-off gas usage as fuel to main propulsion or electric power generation machinery
h)	Azimuth thrusters which are the sole means for propulsion/steering with lubricating oil pumps, cooling water pumps, etc.
i)	Electrical equipment for electric propulsion plant with lubricating oil pumps and cooling water pumps
j)	Electric generators and associated power sources supplying primary essential equipment
k)	Hydraulic pumps supplying primary essential equipment
l)	Viscosity control equipment for heavy fuel oil
m)	Control, monitoring and safety devices/systems of equipment for primary essential services
n)	Fire pumps and other fire extinguishing medium pumps
o)	Navigation lights, aids, and signals
p)	Internal safety communication equipment
q)	Lighting system
r)	Services considered necessary to maintain dangerous spaces in a safe condition
s)	Dynamic positioning systems
t)	Ventilation systems necessary to maintain a safe atmosphere
u)	Elevating (jacking) systems
v)	Ballast control systems (on column stabilized units)

3   Notations

The **CS-System**, **CS-Ready**, **CS-1**, and **CS-2** notations will be assigned upon demonstrating compliance with the requirements given in this Guide.

The scope of the notations is indicated Section 1/Table 2, which outlines the applicability and purpose of each notation.

TABLE 2
CS Notation Applicability

Notation	Applicable to	Purpose
CS-System	Original Equipment Manufacturer (OEM) equipment installed on a specified vessel	Notation documents that at least one of the installed systems, providing a Primary Essential Service, has an active ABS CyberSafety PDA Certificate per 2/1.1 of this Guide. This notation provides OT/IT system information that can be utilized by the Company to satisfy certain **CS-1** and **CS-2** requirements.
CS-Ready	Ship Builder Integrator (SBI) applied to a specified vessel	Notation documents that cybersecurity procedures and protections are applied to critical OT/IT systems during vessel construction and are documented and communicated to the Owner per 2/1.2 of this Guide. This notation provides OT/IT system information that can be utilized by the Company to satisfy certain **CS-1** and **CS-2** requirements.
CS-1/CS-2	Company, Owner, or Vessel Manager applied to a specified vessel	Notation documents that the vessel has met requirements for a cybersecurity program per 2/1.3 of this Guide.

Computer-based control systems within the scope of the **CS-System**, **CS-1**, and **CS-2** notations will be listed in the OT/IT Digital Architecture Description to describe the exact coverage of the applicable notation. For example, 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

For additional information concerning essential control systems, see services considered necessary for continuous operation to maintain propulsion and steering (Primary Essential Services); non-continuous operation to maintain propulsion and steering; a minimum level of safety for the vessel's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services); and, emergency services as described in of the *Marine Vessel Rules* (4-8-1/7.3.3; each service is either primary essential or secondary essential depending upon its nature) and *MOU Rules* (4-1-1/1.1.2, 4-1-1/3.5 and 4-1-1/Tables 3 and 4).

4   Process

4.1   General

To obtain the **CS-System**, **CS-Ready**, **CS-1**, and **CS-2** notations, an engineering review of documentation is required, followed by an implementation survey on board the vessel. **CS-System**, **CS-1**, and **CS-2** require an annual survey to maintain the notation(s). Further, **CS-System**, **CS-1**, and **CS-2** notations require a survey after changes to cyber-enabled, safety-related networked systems, or after a security incident (i.e., cyber-enabled system failure, cyber breach or cyber-attack) that impacts safety-related networked systems.

The **CS-System** notation is unique in that it is granted to a specific vessel for a specific cyber-enabled system that is installed on board that vessel and encourages a full lifecycle collaboration between the system provider and the owner/operator concerning cybersecurity. The **CS-System** notation 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. Further, the notation 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 **CS-System** requirements are the 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 in **CS-Ready**, **CS-1**, and **CS-2** notation requirements and supply chain business arrangements.

The **CS-Ready** notation is unique in that it provides a foundation for **CS-1** and **CS-2** notations by requiring the SBI to collect and compile information provided by system providers and communicate both cybersecurity design and implementation information to the vessel owner or manager (Company). This information is made available to the Company to expedite the process of collecting information required by **CS-1** and **CS-2** notations. To gain the most benefit from the **CS-Ready** notation, the Company may apply for the **CS-1** or **CS-2** notations prior to expiration of the **CS-Ready** notation, which occurs at the first annual inspection of the vessel.

4.2   CyberSafety Reviews

ABS CyberSafety engineering reviews for **CS-System**, **CS-Ready**, **CS-1** and **CS-2** are initiated by the client and follows a uniform process that includes a survey of the implementation on board a vessel.

4.3   Conditions

The given notation is a representation by ABS 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.

4.4   Termination

The maintenance of certification or any notation is conditional upon the continued compliance of the Company and vessel with the requirements of this Guide. Failure by the Company or vessel to continue to comply is grounds for termination of the certification and/or notation.

If ownership or management of the vessel changes, ABS reserves the right to request an additional engineering review and/or implementation survey to confirm that the notation remains current.

4.5   Limitation of Liability

ABS is not liable or responsible in any respect for any inaccuracy or omission in this Guide or any other publication or document issued by ABS. The Company owner, shipbuilder, or commercial operator is responsible for maintaining knowledge of their systems in order to apply security controls and requirements that remedy gaps in system security protections as needed. 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 vessel operation. Refer to Section 1-1-11 of the ABS *Rules for Conditions of Classification, Part 1*.

5   Organizations

5.1   Company

The Company is the Owner of the vessel, or any organization or entity that operates the vessel 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 vessel and initiates a security program or project for the vessel.

5.2 Ship Builder Integrator (SBI)

For a vessel 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 vessel.

5.3 Service Supplier (SS) *(1 August 2023)*

Service Supplier (SS) may be original equipment providers (OEMs) or software development entities responsible for software implemented in the system subject to verification for notation. Verification of integrated systems provided by multiple SSs requires that all SSs participate in the verification process.

5.4 Sub-Supplier (Sub-System or Component Providers) *(1 August 2023)*

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.

6 Definitions and Abbreviations

6.1 Definitions *(1 August 2023)*

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, CNSSI 4009, and ASTM 3286.

ABS CyberSafety®. Guidelines and standards for computerized, automated, and autonomous systems that provide confidence that those systems are designed, built, operated, and maintained to allow only predictable, repeatable behaviors.

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.

Capability. The ability to execute a specified course of action.

Company. See 1/5.1 in this Guide.

Complex Connection. A digital communications path between equipment and a network that supports other digital communications but is not connected to the Internet.

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.

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.

Cyber-Enabled System. Computerized or programmable system built to provide significant degrees of automation in operational function, system monitoring and management, or data communications.

Cyber Event. A detected cyber-related anomaly in a cyber-enabled system.

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.

Cyber Incident. A cyber event that results in the corruption of data or the interruption of service in a cyber-enabled system.

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. (Committee on National Security Systems Glossary, NSSI 4009, 2010)

CyberSafety Service Supplier. An organization that holds a voluntary recognition offered by ABS for qualified suppliers who offer specialized services and enhance existing marine and offshore safety practices and holds an ABS CyberSafety PDA.

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.

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.

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.

Cybersecurity Risk Management System (CRMS). An organizational system that provides technological and procedural cybersecurity protections.

Discrete Connection. A digital communications path characterized by one direct connection (not networked) to one piece of equipment, but not to the Internet.

Documentation. Descriptions, graphical representations, records, and certificates that confirm that the vessel is in compliance with applicable cybersecurity and/or CyberSafety security requirements.

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 vessel's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services), and emergency services as described in 4-8-1/7.3.3 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)* (each service is either primary essential or secondary essential depending upon its nature). Also refer to essential services in 4-1-1/1.1.2, 4-1-1/3.5 and 4-1-1/Tables 3 and 4 of the ABS *Rules for Building and Classing Mobile Offshore Units (MOU Rules)*.

Federated Systems. Systems that work together in an interoperable way that allows data sharing, where each system has separate functionality.

Functions-Connections-Identities™ (FCI™). Patented ABS quantitative risk assessment method for identifying cybersecurity risk contributors of a vessel or facility. FCI analysis informs decision-making concerning application of cybersecurity controls and implementation priorities for cyber risk reduction procedures and technologies and enables relative measurement of cybersecurity risk within and among maritime and offshore vessels.

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.

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.

Industrial Control System (ICS). Computer-based control system for industrial or machinery processes.

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.

Information System. Automated system that enables Company and business process use of data.

Information Technology. Automated systems used for storing, retrieving, processing, and sending data.

Infrastructure. System of facilities, equipment, and services needed for the operation of the Company.

ISM. International Management Code for the Safe Operation of Ships and for Pollution Prevention. Also referred to as the International Safety Management Code.

NIST Cyber Security Framework Core Functions or Elements: Identify, Protect, Detect, Respond, Recover (IDPRR).

Objective. An achievable goal set by the Company stated in terms of the management system's performance.

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.

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.

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.

Remote Access. A method of gaining access to distant vessels 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).

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.

Safety-Critical System. A cyber-enabled component or system installed in a vessel, 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 vessel or to the environment.

Safety Management System (SMS). A structured and documented system enabling Company personnel to effectively implement the Company safety and environmental protection policy. In the CyberSafety 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.

Service Supplier (SS). An organization that holds a voluntary recognition offered by ABS for qualified suppliers who offer specialized services and enhance existing marine and offshore safety practices.

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.

SOLAS Convention. The International Convention for Safety of Life at Sea, 1974, as amended.

Statement of Fact (SOF).   A document that compares the observed state of a cybersecurity risk management system (CRMS) implementation to the cybersecurity requirements provided in this Guide.

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.

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.

6.2   Abbreviations *(1 August 2023)*

CRMS	Cybersecurity Risk Management System
FCI	Functions-Connections-Identities
FDD	Functional Description Document
FMEA	Failure Mode and Effects Analysis
IRT	Incident Response Team
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
OT	Operational Technology
PDA	Product Design Assessment
RO	Recognized Organization
SBI	Ship Builder Integrator
SIEM	Security Information Event Management
SIM	Security Information Management
SIS	Safety Instrumented System
SEM	Security Event Management
SMS	Safety Management System
SS	Service Supplier
TMSA3	Tanker Management and Self-Assessment Best Practice Guide, Third Ed.

7   Plans and Data to be Submitted

ABS engineers review, and surveyors verify documents and implementations that are key to ABS cybersecurity notations as indicated in Section 1/Table 3 of this Guide. Documentation describing these implementation categories is reviewed by ABS prior to an onboard verification survey. This simple, practical approach promotes the completeness of a Company cybersecurity program and supports a comprehensive and efficient ABS 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 vessels, and the cyber-related risks presented by the design, connectivity, and operation of those systems (see Appendix 3).

Risks to critical cyber-enabled systems are contributed to by three fundamental properties: (1) the "if-failed" safety impact of each system on the vessel; (2) vulnerabilities presented in the design of digital networks connecting those systems and the accessibility of related digital endpoints; and, (3) the threats presented by the lack of trust assignable to each person and digital device that can access the digital endpoints. A risk-based cybersecurity risk management system (CRMS) provides protections that mitigate identifiable risk contributions by means of procedures, technologies, and supporting management programs, with each protection being directly traceable to a specific risk contribution.

The documents described in this section are organized in the eight categories introduced above. Complete documentation organized in this patten will accelerate assessment and survey. The requirements for the respective notations are referenced in Section 2 tables of this Guide. The documentation to be provided for ABS Engineering review is listed in this section, is detailed in Section 2, and is organized to describe eight fundamental cybersecurity documents and implementation categories summarized as follows:

i)   *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.

ii)   *Cybersecurity Policies and Procedures.* Policies and procedures that document Company cybersecurity governance and guidance for employees and third parties (e.g., suppliers, contractors, guests).

iii)   *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.

iv)   *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.

v)   *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.

vi)   *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 (Appendix 3).

vii)   *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.

viii)   *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 vessel (see items *iv)*, *v)*, and *vi)* above), but are supported by the remaining five the enterprise-wide documents and activities (see items *i)*, *ii)*, *iii)*, *vii)*, and *viii)* above). Risk assessment and management (see item *v)* above) 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 vessels and individual Company objectives (see Appendix 3/Figure 1).

This approach 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).

This approach also supports a continuous security program for managing evolving critical systems and threat modes, systemic faults/failures, human errors (internal and external cyber events caused by careless errors and negligence), and intentional malicious actions (external hostile criminal acts, espionage, or nuisances).

Maintenance of the notation requires:

● Continuous identification of cybersecurity risk contributors;

● Assessment of those contributors for potential consequences to safety; and,

● Implementation of mitigation controls that are specifically matched to risk contributors, documented, and implemented based on accepted industry practices.

The notation requirements presented in this Guide support NIST cybersecurity guidance, ISM Code recommendations presented in MSC-FAL.1/Circ.3, and International Working Group Guidelines for implementation of a cybersecurity program. The documentation required for each notation is summarized in the following table and detailed in 1/7.1 of this Guide.

TABLE 3
Engineering Document Review *(1 August 2023)*

No.	8 Fundamental Documents of a Cybersecurity Program	CS-System	CS-Ready	CS-1	CS-2
1	Cybersecurity Representative(s) or Organization	Note 1	X	X	X
2	Cybersecurity Policies and Procedures	Note 1	X	X	X[2]
3	Incident Response and Recovery Team	Note 1		X	X
4	OT/IT Digital Architecture Description	X	X	X	X
5	Risk Assessment and Management Plan	X		X	X
6	Cybersecurity Risk Management System (CRMS)	X	X	X	X[2]
7	CRMS Design and Implementation Procedures	Note 1		X	X
8	Management of Change(MOC) Procedures	Note 1	X	X	X[2]

Notes:

1   OEM requirements covered by the ABS CyberSafety Service Supplier recognition (refer to the ABS *Guide for ABS CyberSafety for Equipment Manufacturers – ABS CyberSafety Volume 7*).

2   All **CS-1** requirements and additional requirements concerning Company Policies, CRMS procedures, and MOC procedures are to be met for **CS-2** notation as indicated.

The documentation required in order to receive each of the notations listed below is organized based on the previously described documentation categories.

7.1   CS-System Notation Documentation Submittals *(1 August 2023)*

See 1/4.1 concerning cybersecurity **CS-System** notation requirements and documentation applicable to the OEM during system construction and installation and the following required documentation submittals.

7.1.1   System OT/IT Architecture

Documentation describing the product system architecture.

7.1.2   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.

7.1.3   Installed CRMS Design and Implementation

Documentation describing cybersecurity protective functions embedded in the product, including anti-malware scanning procedures.

7.2   CS-Ready Notation Documentation Submittals

7.2.1   SBI Cybersecurity Representative or Organization *(1 August 2023)*

SBI to provide documentation identifying person(s) responsible for cybersecurity, the organizational location within the SBI, and quality or cybersecurity certificates (e.g., ISO/IEC 27001, ISA/IEC 62443, or ISASecure® certifications).

7.2.2   SBI Cybersecurity Policies and Procedures *(1 August 2023)*

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

7.2.3   Company and Vessel 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 vessel.

7.2.4   Company and Vessel CRMS Design and Implementation Procedures

CRMS functional description document (FDD) detailing the cybersecurity equipment inventory aboard the vessel, a graphical description of that system architecture, and included logical and procedural protections

7.2.5   SBI Management of Change (MOC) Procedures

Documentation detailing change management and configuration control policies and procedures applied during vessel construction, including OT, OT-connected IT, and CRMS software and computer hardware registries.

7.3   CS-1 Notation Documentation Submittals

7.3.1   Company and Vessel Cybersecurity Representative or Organization *(1 August 2023)*

Company to provide documentation identifying person(s) responsible for cybersecurity, the organizational location within the Company, and quality or cybersecurity certificates (e.g., ISO/IEC 27001, ISA/IEC 62443, or ISASecure® certifications).

7.3.2   Company and Vessel Cybersecurity Policies and Procedures *(1 August 2023)*

Company to provide documentation detailing cybersecurity policies and implementation procedures applied to employees, suppliers, and contractors.

7.3.3   Company and Vessel Cybersecurity Incident Response (IR) and Recovery

Documentation describing Company and vessel cybersecurity incident response team(s), including response and recovery responsibilities, capabilities, and staffing.

7.3.4   Company and Vessel OT and Related IT System Architecture

Descriptions and diagrams detailing the OT and connected IT systems architecture that are suitable for performing a physical and cybersecurity risk assessment.

7.3.5   Company and Vessel OT and Related IT Risk Assessment and Management Plan

A cybersecurity risk assessment of the OT and connected IT systems architecture, and a risk management plan derived from that assessment.

7.3.6   Company and Vessel Cybersecurity Risk Management System (CRMS) Design, Operating and Maintenance Procedures

CRMS functional description document (FDD) that includes a functional architecture with an inventory and descriptions of cybersecurity protective equipment; logical and procedural protections (see Appendix 3); operating and maintenance procedures; cybersecurity event/incident corrective/ preventive action procedures; auditing and test procedures; and, change management procedures.

7.3.7   Company and Vessel Cybersecurity Training Program

Documentation detailing cybersecurity training records and training content concerning cyber hygiene and support of specialized cybersecurity functions.

7.3.8   Company and Vessel OT/IT Management of Change (MOC) Procedures

Documentation detailing change management and configuration control policies and procedures applied during vessel operation, including OT, OT-connected IT, and CRMS software and computer hardware registries.

7.4   CS-2 Notation Documentation Submittals

In addition to the submittal requirements noted for **CS-1** notation (1/7.3), the following submittals are required for the **CS-2** notation.

7.4.1   Company and Vessel Policies and Procedures

Documentation detailing additional cybersecurity policies governing network infrastructure management, un-remediated OT cybersecurity vulnerabilities, Ship Master's responsibilities, administrative authorities, and security logs.

7.4.2   Company and Vessel Cybersecurity Risk Management System (CRMS) Design, Operating and Maintenance Procedures

Documentation containing procedures describing if and how cybersecurity responsibilities are shared between IT and OT personnel.

7.4.3 Company and Vessel Management of Change (MOC) Procedures

Documentation detailing management of change procedures governing software change proposals and authorizations, software backup and recovery management, and periodic software verification.

1 Notation Requirements

Section 2/Figure 1 provides a representation of the lifecycle phases for the **CS-System**, **CS-Ready**, **CS-1**, and **CS-2** notations and the CS-PDA Certification. The notations are designed to be complementary and provide full supply chain assessment of CyberSafety for the lifecycle of the vessel. 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.

FIGURE 1
Vessel Lifecycle Application of CyberSafety Certifications and Notations
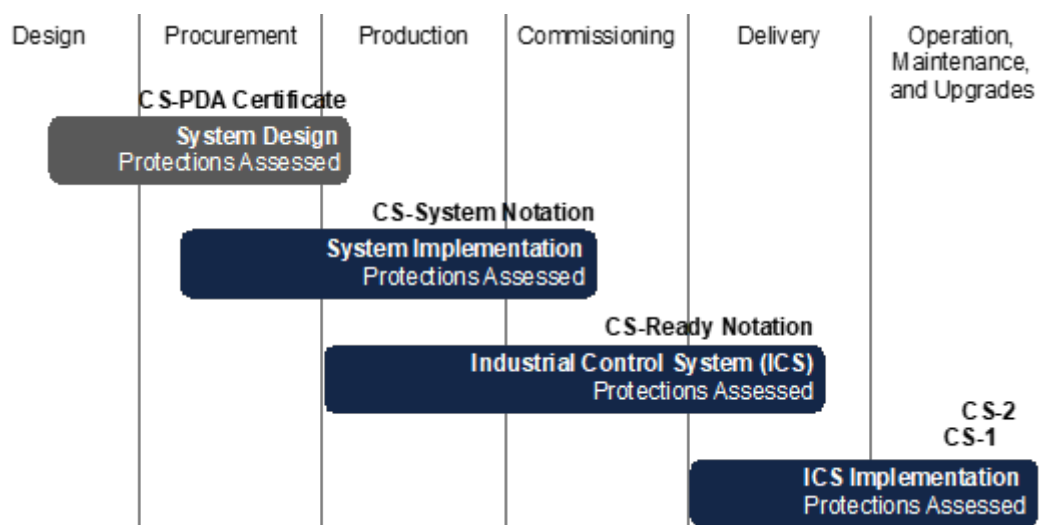
Note: For CS-PDA certification, refer to the ABS *Guide for ABS CyberSafety® for Equipment Manufacturers - ABS CyberSafety® Volume 7.*

1.1 CS-System Notation

The **CS-System** notation (Section 1/Table 2) indicates that the Original Equipment Manufacturer (OEM) has developed, embedded, and described cybersecurity capabilities in the system submitted for notation. 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.

1.1.1 CS-System Notation Requirements *(1 August 2023)*

    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 vessel, 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 ABS (i.e., Design Assessed or Type Approved PDA).

iii)   The OEM system has an active ABS CyberSafety PDA.

iv)   The OEM is to be an active ABS Recognized CyberSafety Service Supplier as defined in Section 2 of the ABS *Guide for ABS CyberSafety for Equipment Manufacturers – ABS CyberSafety Volume 7* and is to satisfy the requirements presented in Section 2/Table 1 and Section 3 of this Guide.

v)   OEM is to deliver system documentation to the shipbuilder during construction, or to the owner/operator upon system installation aboard an operating vessel. The shipbuilder is to maintain system documentation during construction and provide system documentation to the owner/operator upon vessel commissioning. The owner/operator is to maintain the installed system and system documentation during operation in accordance with system provider maintenance agreements.

FIGURE 2
CS-System Notation Requirements Completion Process *(1 August 2023)*
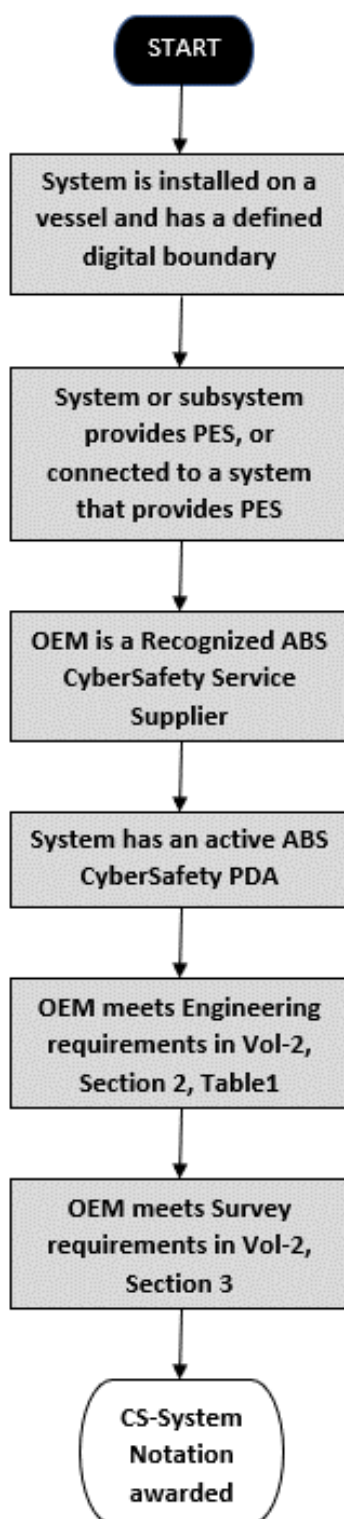
Note: To qualify as a Recognized ABS CyberSafety Service Supplier refer to the ABS *Guide for ABS CyberSafety® for Equipment Manufacturers – ABS CyberSafety® Volume 7.*

TABLE 1
CS-System Requirements for Notation *(1 August 2023)*

#	*ABS CS-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.	ABS CyberSafety Vol-7, Subsection 3/3 **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 (see ABS CyberSafety Vol.7, 1/5.1). ● 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 OEM-provided digitally enabled components (Controlled Equipment List) for each computer-based system included in the ABS PDA (Manufacturer, Model number). ● 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).
		ABS CyberSafety Vol-7, Subsection 3/3 **4 – OT/IT Architecture**

#	ABS CS-System Requirements	References
4	Internal risk assessment of the OEM product(s) is performed and documents: • OT function(s) performed by the system; • Overall Integrity Level (IL) designation (see Section 3/Table 1 of the SQM Guide) as assigned by the OEM, including a description of OT functionality in normal, degraded, and failed states; • Safety FMEA report, if required by other ABS Rules or Guides is documented (If none required, the OEM is to state, "No FMEA required by ABS Rules or 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.	ABS CyberSafety Vol-7, Subsection 3/3 **5 – Risk Assessment & 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.	
7	OEM anti-malware scans performed during final acceptance test for the computer-based system are documented and include name of the vessel on which the scanned system will be installed, scan date, scan results, and anti-malware software name/version number.	ABS CyberSafety Vol-7, Subsection 3/3 **6 – CRMS Design**
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 vessels. • 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 vessels.	

#	*ABS CS-System Requirements*	*References*
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.	ABS CyberSafety Vol-7, Subsection 3/3 **6 – CRMS Design**
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   CS-Ready Notation *(1 August 2023)*

The **CS-Ready** notation is applicable to the Shipbuilder/Integrator (SBI). It establishes requirements for maintaining the integrity of cyber-enabled systems during vessel construction, system integration, and product delivery. During vessel 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 required of Service Supplier by the **CS-System** notation.

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. Note that **CS-System** notation is not a prerequisite for **CS-Ready** implementation. However, documentation required by the **CS-System** notation supports **CS-Ready** notation requirements.

TABLE 2
CS-Ready Requirements for Notation

#	*ABS CS-Ready Requirements*	*References*
1	Identity or identities of the person or persons responsible for cybersecurity during the construction of the vessel are documented and provided to the Company on delivery of the vessel.	ISM Code MSC-FAL.1 /Circ.3, 1.3 NIST CSF: All IWGG Annex 2 **1 – CS Representative**
2	Copies of quality certifications held by the SBI documented and provided to ABS.	
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 vessel.	ISM Code MSC-FAL.1 /Circ.3, 1.5 NIST CSF: Identify, Protect IWGG Annex 2 **2 – Policies and Procedures**

#	*ABS CS-Ready Requirements*	*References*
4	Functional Description Documents (FDDs) of individual systems installed on the vessel 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 vessel. SBI provides the FDD to the Owner/Operator upon vessel 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 vessel. SBI provides the FDD to the Owner/Operator upon vessel 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 vessel CRMS FDD.	ISM Code MSC-FAL.1 /Circ.3, Multiple NIST CSF: Protect, Detect IWGG Annex 2 **6 – CRMS Design**
6	Vessel OT and connected IT equipment and supporting software are to be maintained under revision control during vessel construction and change management records of system updates are to be provided by the SBI to the Owner/Operator upon delivery of the vessel.	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 vessel OT and connected IT systems are to be maintained under revision control during vessel construction and provided by the SBI to the Owner/Operator upon delivery of the vessel.	
8	Vessel CRMS hardware and software are to be maintained under revision control during vessel construction and change management records of system updates are to be provided by the SBI to the Owner/Operator upon delivery of the vessel.	
9	Functional Description Document (FDD) of the vessel CRMS is to be maintained under revision control during vessel construction and provided by the SBI to the Owner/Operator by the SBI upon delivery of the vessel.	

1.3   CS-1 and CS-2 Notations

The requirements for **CS-1** and **CS-2** notations are listed in Section 2/Tables 3 and 4).

TABLE 3
CS-1 Requirements for Notation *(1 August 2023)*

#	ABS CS-1 Requirements	References
1	The cybersecurity risk management system and related program documentation references specific applicable Flag Administration Requirements and international industry standards.	ISM Code MSC-FAL.1 /Circ.3, 1.3 NIST CSF: All IWGG Annex 2 **1 – CS Representative**
2	Government and Flag Administrator requirements and international industry standards concerning contributions to vessel risk presented by cyber-related vulnerabilities and threats are addressed in a risk management plan.	ISM Code MSC-FAL.1 /Circ.3, 2.1.7 NIST CSF: All IWGG Annex 2 **1 – CS Representative**
3	Procedures are documented for identifying non-conformities with cybersecurity-related policies and procedures and correcting related non-conformance issues.	ISM Code NIST CSF: All IWGG Annex 2 **1 – CS Representative**
4	Company policy language committing to manage vessel OT and connected IT cyber vulnerabilities and resulting risks as a priority safety issue is documented.	ISM Code MSC-FAL.1 /Circ.3, 1.4 NIST CSF: Identify, Protect IWGG Annex 2 **2 – Policies & Procedures**
5	Company policy and procedures document management controls concerning failure to comply with policy guidance concerning: • Software maintenance procedures, • Malware scanning procedures, and • Network protection procedures that are prescribed in MOC and CRMS management controls.	ISM Code MSC-FAL.1 /Circ.3, 1.5 NIST CSF: Identify, Protect IWGG Annex 2 **2 – Policies & Procedures**
6	Company policy and procedures conferring administrative authorities for secure access control of vessel OT and connected IT systems are documented.	ISM Code MSC-FAL.1 /Circ.3, 2.2.1 NIST CSF: All IWGG Annex 2 **2 - Policies & Procedures**
7	Company policy and procedures concerning security logging access, use, maintenance, review, collation, and retention are documented.	
8	Procedures that prescribe protective actions to be taken when the disruption of a critical OT and connected IT system is suspected are documented.	ISM Code MSC-FAL.1 /Circ.3, 3.2 NIST CSF: Respond, Recover IWGG Annex 2 **3 – Vessel Incident Response**
9	Procedures for reverting to backups or alternative operational actions when the disruption of a critical OT and connected IT systems is suspected are documented.	
10	A shipboard cybersecurity incident response plan is implemented, documented and included in shipboard emergency plans.	

#	*ABS CS-1 Requirements*	*References*
11	Procedures are documented for identifying and vetting internal and third-party OT and IT technical staff who are responsible for supporting safety-critical cyber-enabled systems. Examples of support staff include but are not limited to personnel technically capable of providing cybersecurity emergency response team (CERT) support to onboard personnel and a designated person ashore (DPA).	ISM Code MSC-FAL.1 /Circ.3, 3.2 NIST CSF: Respond, Recover IWGG Annex 2 **3 – Vessel Incident Response**
12	Procedures are documented for providing access to alternative shipboard communications methods that operate independently of vessel cyber functions to support contact with an incident response designated person ashore (DPA).	
13	Procedures for internally auditing the availability of onboard and DPA emergency cybersecurity incident response resources are documented.	
14	Procedures for implementing alternative modes for operating critical onboard OT and connected IT systems are documented and change management controlled.	
15	An MOC-controlled register documents each cyber-enabled system and portable device on board the vessel and contains: ● System or device description with a unique identifier, ● Person(s) authorized to use or access the system or device, and ● A secure configuration that is approved for the system or device.	ISM Code MSC-FAL.1 /Circ.3, 2.1.2 NIST CSF: Identify IWGG Annex 2 **4 – Vessel OT/IT Architecture**
16	An MOC-controlled register of authorized and unauthorized software installed on board the vessel is documented, maintained, and notes version identifiers and authorized secure configurations.	
17	An MOC-controlled OT and connected IT system architecture description and diagram are documented, maintained, and contains: ● Installed cyber-enabled systems considered to be critical to vessel safety and mission; ● Networked and direct (i.e., non-networked) digital connections with indications of data flows; ● Accessible digital endpoints (e.g., HMIs and ports); ● Identities of personnel having access to digital endpoints; and, ● Identities of portable digital devices connected to or operated near digital endpoints.	
18	Procedures for documenting and updating the equipment registry identifying critical OT and connected IT systems are documented.	
19	Procedures for documenting and updating the software registry identifying critical OT and connected IT applications are documented.	

#	*ABS CS-1 Requirements*	*References*
20	An MOC-controlled cybersecurity risk assessment is documented and references an OT and connected IT system architecture diagram of critical OT and connected IT systems that identifies: ● Software vulnerabilities inherent to critical control systems; ● Digital network connections; ● Digital endpoints characterized as either accessible or not accessible; ● Onboard and remote personnel authorized and unauthorized to access digital endpoints; and, ● Onboard and remote uniquely identified digital devices authorized and unauthorized to access digital endpoints.	ISM Code MSC-FAL.1 /Circ.3, 1.1 NIST CSF: Identify IWGG Annex 2 **5 – Vessel Risk Assessment & Plan**
21	Adjustments that down-scale the CRMS design and (8) supporting cybersecurity program elements for Company applicability are documented and reference reduced scale and complexity of critical OT and connected IT systems as well as reduced scale of risks identified in the risk management plan.	
22	Procedures for routinely validating OEM-provided operational and maintenance information are documented.	ISM Code MSC-FAL.1 /Circ.3, 1.2 NIST CSF: Identify, Protect IWGG Annex 2 **6 – Vessel CRMS Design**
23	Procedures for responding to and reporting unauthorized access to critical OT/IT systems and networks, unauthorized use of administrative privileges, and suspicious network activities are documented.	
24	Procedures for responding to and reporting unauthorized use of removable media, portable media, and personal digital devices are documented.	
25	Procedures for reporting and documenting disruptions in the availability of critical systems or loss of the availability of data required by critical systems are documented.	
26	The Ship Master's responsibilities and authorities for compliance with cybersecurity policies and procedures are documented.	
27	Cybersecurity controls implemented to protect critical OT and connected IT system endpoints from connection by unauthorized or untrained personnel, and in situ, remote, and portable digital devices and media are documented.	ISM Code MSC-FAL.1 /Circ.3, 2.1.1; 2.1.9 NIST CSF: Identify, Protect IWGG Annex 2 **6 – Vessel CRMS Design**
28	Procedures for protecting and routinely verifying the integrity of data essential to cybersecurity risk management are documented.	ISM Code MSC-FAL.1 /Circ.3, 2.1.9 NIST CSF: Protect, Detect IWGG Annex 2 **6 – Vessel CRMS Design**
29	Security logs for monitoring critical OT and connected IT systems with embedded security logging capabilities are enabled, maintained, and periodically reviewed.	
30	Registers of equipment and software authorized for use aboard the vessel are documented and contain: ● Identification of the data processed/stored by listed equipment, and ● User access requirements operational access criteria (i.e., need to access).	ISM Code MSC-FAL.1 /Circ.3, 3.1 NIST CSF: Identify, Protect, Detect IWGG Annex 2 **6 – Vessel CRMS Design**

#	*ABS CS-1 Requirements*	*References*
31	Logical (i.e., technological) and procedural CRMS risk mitigation controls are documented in the CRMS design, verifiable in the CRMS implementation, and directly traced to risks identified in a cybersecurity risk assessment and risk management plan.	ISM Code MSC-FAL.1 /Circ.3, 3.5 NIST CSF: All IWGG Annex 2 **6 – Vessel CRMS Design**
32	Cybersecurity policy and procedure compliance training is documented, is provided to onboard personnel, and includes Ship Master's authorities and responsibilities for compliance.	ISM Code MSC-FAL.1 /Circ.3, 2.1.5 NIST CSF: Protect IWGG Annex 2 **7 - Training**
33	On-going company-wide cybersecurity awareness and procedures training is documented and provided based on formal training requirements and incorporated in the general training curriculum.	ISM Code MSC-FAL.1 /Circ.3, 3.6 NIST CSF: All IWGG Annex 2 **7 - Training**
34	On-going specialized cybersecurity training is documented and provided for personnel responsible for implementation and maintenance of CRMS processes.	ISM Code MSC-FAL.1 /Circ.3, 3.6 NIST CSF: All IWGG Annex 2 **7 - Training**
35	Training for IT and OT staff is documented and contains the following training information: • Impacts on personnel and environmental safety caused by disruptions in critical IT and connected OT system functionality; • Guidance on recognizing cyber risk contributors; and, • Responsibilities of IT and OT personnel for collaboratively applying cybersecurity technologies and procedures to IT and connected OT systems.	ISM Code MSC-FAL.1 /Circ.3, 3.7 NIST CSF: Identify, Protect IWGG Annex 2 **7 - Training**

#	*ABS CS-1 Requirements*	*References*
36	MOC and configuration management control procedures document: • Accurate descriptions of OT and connected IT system configurations; • Proposed equipment installations/removals; • Proposed software installations/removals; • Proposed alterations in data flows; and, • Proposed revisions in the OT and connected IT system architecture diagram.	ISM Code MSC-FAL.1 /Circ.3, 2.1.8 NIST CSF: All IWGG Annex 2 **8. Management of Change**
37	MOC procedures document: • Maintenance of software security (e.g., "patching"); • Information integrity checking; • Configuration control of software and devices (i.e., "secure" settings); and, • Routine operation of OT and connected IT systems.	
38	Procedures for authorizing remote and onboard digital access to OT and connected IT systems and verifying service supplier (OEM) adherence to Company change management processes are documented.	
39	Procedures for requiring service suppliers to comply with configuration and change management controls that prohibit the use of uncontrolled (i.e., unscanned or potentially corrupted) portable media when performing software updates are documented.	
40	Procedures for restricting OT and connected IT system software maintenance activities to vetted Company personnel who have administrator-level access credentials are documented.	

TABLE 4
CS-2 Requirements for Notation

(Completion of both **CS-1** and **CS-2** requirements are required for **CS-2** notation)

#	*ABS CS-2 Requirements*	*References*
1	Company policy prioritizing the importance of cybersecurity risk management as being equal to other identified corporate risks is documented.	ISM Code MSC-FAL.1 /Circ.3, 3.2 NIST CSF: Respond, Recover IWGG Annex 2 **2 – Policies & Procedures**
2	Company policy governing unremediated OT and connected IT cybersecurity vulnerabilities that potentially disrupt safe operation of maritime and offshore vessels is documented.	
3	Company policy governing security protections for cyber risk management of OT and connected IT systems and related network infrastructure is documented.	
4	Company policy and procedures governing the use, organization, maintenance, retention, and periodic review of security logs by authorized employees are documented.	

#	ABS CS-2 Requirements	References
5	Company policy and procedures governing the reporting of disruptions in critical system availability or loss of the availability of data required by critical systems are documented, periodically reviewed, and maintained.	ISM Code MSC-FAL.1 /Circ.3, 1.2 NIST CSF: Identify, Protect IWGG Annex 2 **2 – Policies & Procedures**
6	Procedures are documented, periodically reviewed, and maintained for identifying and vetting internal and/or third-party IT/OT technical personnel capable of supporting onboard safety-critical cyber-enabled systems, onboard IT/OT personnel, the cybersecurity emergency response team (CERT), and cybersecurity designated person ashore (DPA).	ISM Code MSC-FAL.1 /Circ.3, 1.2 NIST CSF: Identify, Protect IWGG Annex 2 **6 – Vessel CRMS Design**
7	Procedures describing how responsibilities for designing, implementing, and maintaining the CRMS are shared between IT and OT personnel and documented.	ISM Code MSC-FAL.1 /Circ.3, 2.1.9 NIST CSF: Protect, Detect IWGG Annex 2 **6 – Vessel CRMS Design**
8	Installation of software back-ups to recover functionality of critical onboard OT and connected IT systems is restricted to authorized personnel and documented in change management procedures.	ISM Code MSC-FAL.1 /Circ.3, 2.1.8 NIST CSF: All IWGG Annex 2 **8 – Management of Change**
9	Proposed revisions to critical OT and connected IT systems and networks are authorized through and documented in a change management procedure that includes analysis of cybersecurity vulnerabilities, review of secure configuration settings, and updates in system architecture diagrams.	
10	Periodic data integrity verifications are performed on data sets used by critical OT and connected IT systems by comparing "current state" information to "known-good state" criteria, and resulting revisions to data sets are documented in change management records.	
11	Permissions to access locally and remotely stored software back-ups of critical OT and connected IT system software and data sets are documented change management procedures.	
12	Procedures for periodically auditing process instructions for accessing, backing up, recovering, restoring, and testing critical onboard OT and connected IT systems are documented in change management records.	

1 General

This Section outlines the Class survey requirements for the **CS-System**, **CS-1**, and **CS-2** notations. Vessels under construction are eligible for the **CS-System** and **CS-Ready** notations. Operational vessels are eligible for the **CS-System**, **CS-1**, and **CS-2** notations. The scope of survey will include the critical systems defined in the engineering approval letter.

2 Surveys During Construction

2.1 CS-System Initial Surveys *(1 August 2023)*

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 vessel 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 vessel.

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

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

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   CS-Ready Initial Surveys

The Surveyor is to verify SBI physical security and change management policies and procedures applied during vessel 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 vessel.

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 ABS.

viii)   SBI documentation that describes installed cybersecurity functions.

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

2.3   CS-1 and CS-2 Initial Surveys *(1 August 2023)*

For the **CS-1** or **CS-2** notation, documentation submissions (Subsection 1/7) are to be provided for surveys of notation requirements detailed in Section 2/Tables 3 and 4, respectively.

Initial survey is to be carried out for the **CS-1** or **CS-2** notation following the issuance of an engineering approval letter.

The initial verification survey is to be performed on board the vessel to confirm that the following are documented and implementation-verified to the satisfaction of the attending Surveyor:

i)   Vessel cybersecurity risk management system (CRMS) (Appendix 3);

ii)   Processes and programs detailed in Section 2/Tables 3 and 4, as applicable;

iii)   Maintenance procedures supporting Company-required maintenance of OT systems, IT systems, and CRMS protections as detailed on OEM solution provider documentation; and,

iv)   Vessel-specific cybersecurity programs and capabilities including:

    a)   Functional Design Document description (Appendix 2);

    b)   **CS-1** Requirements listed in Section 2/Table 3; and,

    c)   **CS-2** Requirements listed in Section 2/Table 4.

Cyber risk management systems that have been surveyed to the satisfaction of the attending Surveyor to the full requirements of this Guide as applicable, where approved by the Committee, may be classed and distinguished in the ABS *Record* by the notation **CS-1** or **CS-2**.

3   Surveys After Construction *(1 August 2023)*

For requirements for surveys after construction, see Section 7-9-46 of the ABS *Rules for Survey After Construction (Part 7)*.

4   Modifications (Any Notation)

4.1   General

The Company is to advise ABS Engineering of modifications to cyber-enabled equipment installations and/or changes made to OT and connected IT systems, and cybersecurity protective controls that impact the requirements stated in this Guide. The Company is also to submit to ABS Engineering details concerning revisions in OT and connected IT systems and CRMS architecture descriptions, as applicable to the specific notation including:

i)   Addition or removal of a critical system from the CyberSafety notation.

ii)   If changes or upgrades to the CRMS that alter conformance to ABS requirements, an additional survey may be carried out at the discretion of ABS to confirm that implementation of the modification or management system meets ABS requirements.

Note: Examples of changes sufficient to compel a reassessment of a cyber-enabled, safety-related networked system includes a major change in either OT or IT safety-relevant systems; control system changeouts in safety-critical systems; or, combined configuration changes between or among two or more systems that control safety-critical systems. Other examples that also apply include security events that affect safety related or mission-critical functions or systems.

4.2   Revisions of CRMS

The Company is to advise ABS of changes made to the cyber-enabled equipment/software registries and architectures and/or cybersecurity protective controls following vessel delivery and upon application for the **CS-1** or **CS-2** notation. Based on this notification, ABS will determine if a new survey is required.

5   Partial Compliance (Any Notation)

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

Maritime Cybersecurity Risk Assessment

1   General

This Appendix is included to provide guidance on the risk assessment process applicable to cybersecurity.

2   Risk Assessment Process

Risk assessment represents the technical core of Cybersecurity Risk Management. Cyber risk can be represented as an interaction of three risk elements: (1) the consequences of a cyber-incurred failure; (2) cyber-related vulnerabilities that enabled the failure; and (3) cyber-related threats that incited the failure.

These three risk elements originate from risk contributors affecting:

1)   Critical cyber-enabled OT systems and related IT systems;

2)   Digital infrastructures supporting critical cyber-enabled OT and related IT systems; and,

3)   Identifiable personnel and digital devices that access OT systems.

Digital systems are threatened by untrusted humans and digital devices that access digital connections through vulnerable endpoints (i.e., ports and HMIs) and deliver threat "modes" (e.g., malware, viruses, ransomware, etc.) to cyber-enabled systems. This model can facilitate identification of risk contributors that can be identified, qualified, quantified, and prioritized for implementation. Further, needed cyber protections can be selected based on analysis of these risk contribution types.

A risk-based approach to cybersecurity calls for the Company to identify contributions to risk to facilitate prioritization of risk mitigation efforts, establish security rules and practices, and select security technologies and methods. The following characteristics are included in the overall risk assessment process:

i)   Designation or prioritization of automation functions (equipment) as being critical to vessel safety and mission completion;

ii)   Characterization of cyber risk contributors based on the following:

- Digital design of each critical function;
- Type and accessibility of each digital endpoint; and,
- Trustworthiness of each person and digital device allowed to access each digital endpoint;

iii)   Risk management controls as represented in selected cybersecurity guidance that can reduce risk by controlling each risk type (i.e., function, connection, and identity risk types);

iv)   Business decisions concerning risk avoidance, transference, acceptance, or mitigation; and,

v)   A risk management plan that specifically informs risk management control selections.

A risk assessment is performed in two parts:

i)   A "tabletop" assessment referencing the critical OT system architecture description, technical diagram, and related functional description documents; and,

ii)   A shipboard assessment to verify the documented description of the OT system architecture and detail observed characteristics of risk contribution types.

A risk assessment approach, whether quantitative or qualitative, directly relates risks identified with risk mitigation choices presented in the risk management plan. The methodology contains the following information:

i)   Uniform process instructions that are followed for risk assessment and management activities.

ii)   References to formal enterprise guidance (e.g., documented policies and procedures) governing risk management activities.

iii)   References to rigorous change controls (e.g., management of change (MOC)) indicating periodic updates reflecting the current threat (risk) environment.

iv)   A list of stakeholders actively involved in risk management activities, as well as those directly involved in any risk assessment or mitigation workshops that are conducted.

v)   A description of how risk analyses are informed by network (OT/IT) architecture design documentation.

vi)   Objective risk criteria used for evaluating, categorizing (i.e., a taxonomy), and prioritizing operational risks based on impact, tolerance for risk, likelihood of occurrence, and risk response approaches.

vii)   Quantitative risk prioritization analyses, if reference databases are satisfactorily robust to contain the systems under review for meaningful and relevant results.

viii)   Specific risks observed on the vessel(s) during risk assessments.

ix)   Support information of a "risk register" (e.g., a structured repository) of identified and classified risks used to support risk management decisions.

x)   Analyses for prioritizing risk response implementations contained in Cybersecurity Risk Management System (CRMS) designs.

xi)   Specify control treatments anticipated or implemented in the CRMS for each risk (i.e., mitigated, accepted, tolerated, or transferred).

xii)   Reciprocal traceability between risks identified in the risk assessment and mitigation methods/ controls maintained and instantiated in the CRMS design.

Industry best practices include documentation of a Risk Management Plan informed by identified OT cybersecurity risks to critical functions listed in the industrial control system FDD. This activity is an assessment of observed on-vessel risk contributors and their specific characteristics followed by the creation of a "risk taxonomy."

Architectural analysis directly uses a risk taxonomy in the context of systems inventory, as inputs to a quantitative risk assessment, such as the ABS Functions-Connections-Identities™ (FCI) model. A quantitative assessment allows prioritization of risk treatments and mitigation actions that follow from the 12-step risk assessment approach above.

A Failure Modes and Effects Analysis (FMEA) for critical systems or functions informs the analysis process, if available. The risk assessment also verifies implementation of planned or in-place control types for managing the specific observed risks.

The Risk Management Plan provides requirements for Cybersecurity Risk Management System (CRMS) design activities that are directly traceable to CRMS control solutions. The risk assessment and resulting Risk Management Plan documents govern and inform CRMS design activities guided by the topics listed in the risk assessment paragraph above. The CRMS is discussed in detail in Section 3 of this Guide.

This progression of risk management activity uses complementary qualitative (survey and goals/objectives/ tasks requirements) and quantitative methods to develop a complete vessel risk profile. A quantitative analysis is used to complete the risk profile for a vessel.

1 Functional Description Document (FDD)

The purpose of the FDD is intended to provide an accessible revision-controlled document containing a description of the CRMS equipment and security applications in a form readily understandable by shipboard personnel who are authorized to access proprietary CRMS information and who are responsible for evaluating, auditing, operating, or maintaining that system.

The FDD is intended to be a documented engineering description of the CRMS equipment and software. Its primary function is to provide operations, maintenance, and evolution (updating) guidance for the CRMS. In the cybersecurity context, this function provides a view of the systems to be protected as a basis for developing a risk assessment and risk management plan that inform a risk-type taxonomy and remediation selection process. The FDD also

- Provides *evidence of engineering rigor* to class societies and regulators;
- Provides information needed to control or resolve *cybersecurity system failures* directly and quickly; and,
- Assists in identifying Predicts *potential cascading failures of protected control systems*

Information sources for creating the FDD include external specialists who collaborate to develop the CRMS as well as internal support staff. In that the design and implementation details of the CRMS are typically restricted and confidential, sources are to be those personnel authorized to have access to CRMS design and operational information.

The suppliers or internal technical staff responsible for engineering control system functionality and implementing cybersecurity and related physical systems are the primary providers of FDD content. Subsuppliers of supporting technologies and applications (e.g., CRMS networks, protection monitors, software applications) may provide FDD information as well. The system integrator (e.g., the shipyard) may also provide information about the overall system structure or the architectural context of the installed security system. In creating the FDD, information may be required from multiple providers. Accordingly, such information may be held in multiple locations. Relevant information may be in the possession or control of the Company or operator.

1.1 FDD Described in Four Main Parts *(1 August 2023)*

The vessel FDD content includes four (4) main parts:

1) *Description:* Functional description of the systems for which the CyberSafety Management System (CRMS) defines risk management rules, controls, and activities.

2) *Safety:* Review of safety impacts of the CRMS on protected ICS and computer-controlled equipment.

    3)   *Test:* Pre- and post-installation test procedures for the systems to which CRMS applies.

    4)   *O&M:* Operation and Maintenance procedures for the systems to which CRMS applies, including change management.

The FDD aggregates technical and operational knowledge of cyber-enabled systems on board the vessel. To that end, the FDD is intended to contain content that aids ship's engineers and crew to understand the ship's systems, including, but not limited to:

    1)   *General and specific description for each cyber-enabled function (cybersecurity subsystem functions):*

          a)   An engineering technical diagram (set) of the ICS and cyber-enabled network(s) indicating network segmentation (as applicable);

          b)   An engineering technical diagram (set) indicating the cyber-enabled subsystems protected and enabling connections (interfaces);

          c)   An engineering technical diagram (set) of the cyber-enabled systems monitoring locations, including monitoring and analysis technologies (devices) deployed;

          d)   A listing of machine and human identities (roles) authorized to access the CRMS system(s); and,

          e)   A description of the processes (methods) implemented to verify and validate identities (roles) authorized to access the CRMS system(s).

    2)   *Safety review for each of the CRMS subsystem functions, accompanied by an Integrity Level (IL) (0, 1, 2, or 3) designation:*

          a)   An assignment of an IL rating to the major functions of the systems within CRMS, or to the full system (see the ABS *Guide for Software Quality Management (SQM)* for detailed discussion of IL determination and designation); and,

          b)   An analysis of the impact of failed and degraded CRMS systems' conditional states on the ICS:

               i)   If a failure of the cybersecurity function can cause a related failure of an ICS function that the CRMS function is monitoring and/or protecting, the CRMS function inherits the IL rating of the protected ICS function.

               ii)   If the CRMS function cannot cause a failure of the protected ICS function being monitored or protected, the CRMS function may be assigned an IL rating as collaboratively agreed by the supplier and/or the Company (owner of the vessel).

               iii)   If the protected ICS function that can be caused to fail by the CRMS function is designated as a Safety Instrumented System (SIS), the CRMS function inherits the SIS designation of the protected system.

    3)   *Test (i.e., CRMS final test plan, test results, with resolution of test issues or findings) for each CRMS function:*

          a)   A test plan that includes test procedures for final functional test of the FDD system as implemented; and,

          b)   Documented FDD system test results, including corrections to the CRMS based on the test outcomes.

    4)   *Operation and maintenance information for each CRMS function (i.e., security capability) as provided by the supplier or internal implementation team:*

          a)   A listing (registry) of the security components and applications of the CRMS;

          b)   A management of change system that governs changes and updates in the CRMS, including post-installation regression test requirements; and,

c)   CRMS operations and maintenance documentation provided by the supplier or internal development team.

Cybersecurity Risk Management System (CRMS)

1 Cybersecurity Risk Management System (CRMS)

1.1 Background of Maritime Cybersecurity and the ABS Approach to Assessment

The NIST Cyber Security Framework identifies five functions that represent eight activities that describe the mechanics of a cybersecurity program. In this approach (see Subsection 1/7) to assessing maritime cybersecurity programs, activity #6 represents the CRMS. The CRMS is comprised of a collection of specialized procedural and technological security controls focused on cyber-enabled operational systems aboard the vessel. The remaining 7 activities are performed in service of the CRMS. That is, if the 7 non-CRMS activities are performed at a very high degree of proficiency, CRMS controls are supported over time and may arguably be reduced. The CRMS augments human cybersecurity capabilities in much the same way that electromechanical systems augment human strength and awareness.

Readily available CRMS technologies augment cybersecurity through means that extend beyond the human ability to Identify, Protect, Detect, Respond to, and Recover from a cybersecurity incident. However, since most cybersecurity events occur because an authorized person failed to follow procedures for the secure use of cyber-enabled systems, CRMS technologies should be considered as tools that extend the human ability to protect essential systems rather than replacements for those abilities. This appendix provides insight into the ABS view of CRMS characteristics, design, implementation, maintenance, and evolution. It also provides information concerning the more unique characteristics of a maritime CRMS.

ABS considers the CRMS as an engineered system. As such, the CRMS design is based on clear engineering requirements developed to manage cyber risk. Cyber risk is defined by a unique form of "physics" comprised of three properties of risk associated with computerized control (i.e., Operational Technology, or "OT") systems: Consequence, Vulnerability, and Threat. If any one of these elements is not present or is reduced in value, then cyber-related risk is not present or is likewise reduced in value. The goal of the CRMS is to eliminate or lessen risk based on these three properties. Therefore, the *role of the CRMS designer* is to select and implement organizational, technological, or procedural controls that specifically work to manage these cyber risk properties when those properties cannot be successfully managed.

The *engineering of a CRMS* is done within a cyber environment that is not manageable by applying means listed above. The requirements for the design of that system are collected by performing a risk assessment that acknowledges the three properties of cyber risk. ABS recognizes these cyber risk properties for vessels as transforms that are observable and quantifiable as:

- *Consequential vessel FUNCTIONS* limited to Primary Essential Services and digitally connected information technology systems;

- *Vulnerability of FUNCTIONS* limited to digital CONNECTIONS represented as physical (i.e., wired and wireless) and software endpoints; and,

● *Threats to FUNCTIONS* limited to IDENTITIES of persons and wired or wireless digital devices under human control that have onboard or remote access to FUNCTIONS through digital CONNECTIONS.

Access to a consequential function and the intentional or unintentional agenda of an identity to introduce a threat mode (i.e., malware in the general sense) into that function "closes the circuit" to create a cybersecurity risk. The CRMS augments the ability of a vessel's crew and shoreside staff to recognize, prevent, and recover from that event. The requirements provided in this Guide are based on that idea. At the most general level, ABS evaluates the:

● Accurate identification of Primary Essential Services and related IT functions on board and digitally connected to a vessel;

● Accurate observation and classification of risk properties;

● Accurate application and traceability of risk properties to risk management controls implemented in the CRMS; and,

● Sufficiency of the seven (7) activity/documentation areas that concurrently operate in service of designing, implementing and maintaining a functional CRMS.

1.2 ABS Model for Cybersecurity Engineering Review and Survey

The following model depicts how ABS evaluates the application of risk assessment analysis to cyber risk management program outcomes in a practical sense. This model indicates how ABS expects and encourages the user Company to select and apply "best fit" cybersecurity controls guidance to its program and assume responsibility for scaling the implementation of its cybersecurity program activities and documentation so as to make the program and resulting CRMS implementation appropriate to its business size and goals. At the same time, regardless of the scale of implementation, ABS expects a user Company to include all eight activities and related documentation enumerated in the model, with the understanding that activities #4 through #6 are core vessel-specific CRMS activities, while activities #1 through #5, and activities #7 and #8 are required to maintain a sustainable and evolving CRMS implementation.

FIGURE 1
ABS Engineering/Survey Cybersecurity Architecture Model
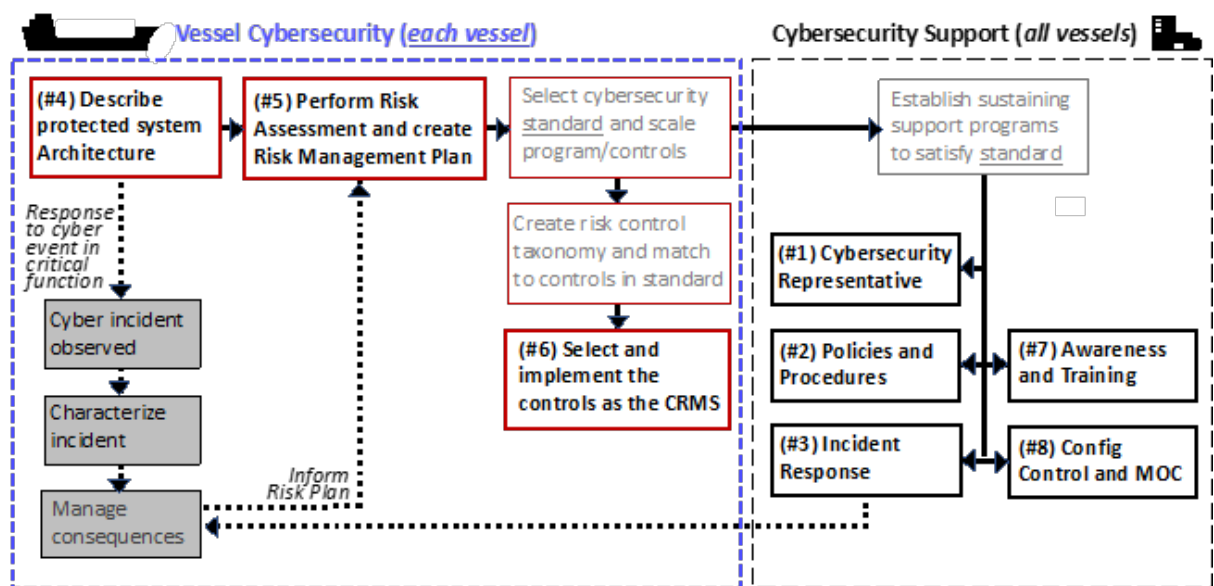
1.3   Organizational Cybersecurity Best Practices

CRMS design documents guide and prioritize efforts to select and improve both procedural and technological organizational cybersecurity capabilities to meet enterprise security needs. The following activities are addressed at the organizational level. These activities represent organizational competencies as well as standing activities and system documentation matured over the lifetime of the cybersecurity program defined in Subsection 1/7 in this Guide and listed below.

i)   *Cybersecurity Representative(s) or Organization.*

ii)   *Cybersecurity Policies and Procedures.*

iii)   *Incident Response and Recovery.*

iv)   *OT/IT Digital Architecture Description.*

v)   *Risk Assessment and Management Plan.*

vi)   *CRMS Design and Implementation Procedures.*

vii)   *Cybersecurity Training Program.*

viii)   *Management of Change (MOC) Procedures.*

Seven of the eight activities listed above functionally support the design, implementation, ongoing operation, and evolution of activity *vi)* above: the design, implementation, maintenance, and evolution of the CRMS (#6 in the graphic). Listed below are general cybersecurity considerations performed at the organizational level as assigned to personnel responsible for the above eight activities.

i)   Evaluation of acceptable cybersecurity risk for the enterprise may include the following activities:

   a)   Definition of cyber-related risk properties, contributors, impacts posed by external and internal threats to vessel safety and organizational mission;

   b)   Prioritization of risk mitigation control implementation based on risk contributor types;

   c)   Assessment and certification of system, vessel, facility and enterprise CRMS performance; and,

   d)   Assessment of incident response and recovery capability that supports vessel safety and enterprise mission.

ii)   Evaluation of sufficiency of protective measures and controls for the vessel and enterprise may include the following considerations:

   a)   Communications among OT system perimeter protection and monitoring devices and enterprise log management or SIEM system(s);

   b)   Use of situational awareness tools (i.e., digital dashboard) to represent security, perimeter protection, and monitoring systems;

   c)   Consolidation of OT system communication paths to simplify communications traffic filtering and monitoring;

   d)   Use of web application protections (i.e., firewalling);

   e)   Use of host-based protections for connected IT systems that report through monitoring dashboards;

   f)   Recurring training for security personnel concerning security monitoring procedures and metrics;

   g)   Software backups for workstations and data stores maintained in protected, segregated storage;

   h)   Enterprise personnel records and entities maintained under enterprise identity and access management control;

i)   Software integrity testing throughout the lifecycle of the control system;

j)   Change management procedures that include configuration control, vulnerability evaluation, and rigorous patch management processes;

k)   Configuration, vulnerability, and patch management processes performed in consideration of threat and threat mode research to establish update prioritizations and feedback to risk management authorities;

l)   Initial configuration of enterprise system based on and managed through security guidelines provided by configuration control and change management procedures; and,

m)   Routine management of OT and IT systems based on documented procedures.

iii)   Evaluation of physical locations for systems and data may include the following considerations:

a)   Security and redundancy of data center(s) and disaster recovery facilities;

b)   Security of physical facilities and document stores;

c)   Enhancement of security through distributed digital data stores within facilities;

d)   Creation of data siloes with limited external accessibility;

e)   Protection of or limited access to digital endpoints and restrictions on the use of removable media; and,

f)   Physically protected storage locations for media and data.

iv)   Identification of, authorization of use, and authorized configurations for mobile devices and storage (phones, portable computers, and USB storage devices) may be considered.

v)   Identification and characterization of logical (i.e., computational) locations for data may be considered, including the following:

a)   Digitally connected mobile or stationary computational devices;

b)   Digitally connected shared or segregated data storage devices ("drives");

c)   Collaborative data in storage devices:

1)   OT/IT data in storage devices that are collaboratively accessible, including "Cloud" service devices;

2)   OT/IT data in storage applications that are collaboratively accessible (e.g., SharePoint), including "Cloud" software services; and,

d)   Inactive data storage devices (e.g., backup and archived data sets).

vi)   Categorization of personnel roles and rules for on-site and remote data access may be considered, including the following:

a)   Roles

1)   Active or retired employee

2)   Contractor, consultant

3)   Customer

4)   Supplier

5)   Public

b)   Rules

1)   Project authorizations

2)   Need-to-know

3)   Minimum privilege

        4)   Separation of duties

    c)   Exceptions and special cases

        1)   System administrator accounts

        2)   Service accounts

        3)   Test accounts

        4)   Developer accounts, especially when geographically remote.

2   CyberSafety Risk Management System Relationship with Safety Management System

2.1   General

2.1.1   Cybersecurity Safety Objective Considerations

The Company establishes, implements, and maintains programs or activities for achieving its cybersecurity business objectives. These objectives take into account the unique design characteristics and operating requirements of each ship's type and cyber-enabled systems. For more information, refer to ISM Code Part A, Implementation, Section 1.2, Objectives.

2.1.2   Implementation of Functional Requirements

The Company determines the protections and procedures needed for the CRMS and their application aboard each vessel and throughout the Company. The Company determines the implementation sequence and interaction of these processes. For more information, refer to ISM Code Part A, Implementation, Section 1.4, Functional Requirements for a Safety Management System.

2.1.3   Recommended Cybersecurity Program Activities and Best Practices

See also A3/1.3 and Subsection 1/7 of this Guide.

i)   Designate responsibility for cybersecurity programs to an individual or team.

ii)   Establish Company policy governing cybersecurity programs that is on the same level of importance as other safety-related policies.

iii)   Establish an incident response and recovery program and team with cross-organizational recovery skills that is responsible for shoreside and onboard cyber-related incidents.

iv)   Define the individual OT systems and integrated OT system architectures considered critical to safety within the Company and aboard Company vessel. Develop system architecture diagram of the system or systems that is suitable for a tabletop cyber risk assessment.

v)   Perform a risk assessment of systems defined in item A3/2.1.3iv) above and develop a cyber risk management plan for controlling each risk contributor documented in the risk assessment.

vi)   Develop a CRMS design that makes each design element traceable to each risk contributor documented in the risk management plan. Implement the CRMS design based on the requirements defined in the risk management plan.

vii) Establish a training program for Company and third-party personnel in cybersecurity responsibilities and remedies for non-compliance with policies and procedures, as well as operations and maintenance of the CRMS.

viii) Establish a configuration control and change management program and procedure that maintains the accuracy of the architecture diagram defined in item A3/2.1.3iv) above and Subsection 1/7 of this Guide.

2.1.4   Recommended Documentation of Company Responsibility for Outsourced Programs

When the Company "…chooses to outsource any process that affects product conformity to requirements, the Company confirms control over such processes. The type and extent of control to be applied to these outsourced processes shall be defined within the management system". (ISO 9001:2015, 4.1)

2.2   Cybersecurity Risk Management System

The Company describes the pertinent cybersecurity-related protection program safeguards and the impacts of those safeguards on critical system security. CRMS documentation reflects accommodations of the ISM Code structure for a Safety Management System and contains the following information:

i)   *Defines and documents the scope of the CRMS,* including details and justifications for exclusions based on risk acceptance, avoidance, mitigation and transfer.

ii)   *Includes pertinent Company policies and objectives.*

iii)   *Defines the responsibility, authority, and interrelation of the Company authorities and the operational personnel* who manage, perform, and verify work relating to and affecting cyber-physical system security or cybersecurity, safety operations, or environmental effects, as appropriate.

iv)   *Defines the Master's responsibilities and authorities* for shipboard systems and for connections to offboard systems, in the context of safety requirements for ship operations.

v)   *Describes the resources, core elements and the functional architecture* of the Company's CRMS and interaction of its elements, with references in related documents. Documents identifying risks assessed and mitigating actions taken to address those risks are included in CRMS design documentation.

vi)   *Includes documented procedures established for the Cybersecurity Risk Management System* or provide appropriate references to Cybersecurity Risk Management System documentation. The complexity of the work and the work environment, and the skill level of personnel involved in performing the work are governed by the degree of control provided within management system procedures for shipboard operations and maintenance.

vii)   *Describes the interaction between the processes of the Cybersecurity Risk Management System,* indicating any dependencies or critical enabling factors that must be considered. Include emergency preparedness requirements for cyber-enabled system failures that can result in safety hazards or incidents.

viii) *Includes the procedures and records required by this Guide* to demonstrate conformity to CyberSafety capability requirements and the effective planning, operation, audit, and control of the Cybersecurity Risk Management System processes. Procedures for nonconformity reports, cyber incidents and events, and remediation requirements are addressed.

ix)   *Includes documents and records, determined by the Company to be necessary,* to demonstrate the effective planning, operation, and control of processes and systems that relate to the Company's significant CyberSafety aspects, including management of its cybersecurity risks to both IT and OT systems.

x)   *Supports Company use, verification, review, and evaluation of CRMS processes and procedures.* The Cybersecurity Risk Management System, the Risk Management Plan and/or in the Functional Description Document (FDD) provide the Company with a complete understanding of its cyber-enabled systems, their operational capabilities, and the modes and methods by which the risks of those systems to ship, personnel and environment are managed.

2.3   Resources, Roles, Responsibility, Accountability, and Authority

The Company assigns cybersecurity management resources, defines roles, and assigns responsibilities based on documented criteria. Example criteria are presented below.

2.3.1 Resources

i) The Company's management determines and provides the resources essential to:

a) Establishing, implementing, maintaining, and improving the CRMS;

b) Personnel interacting with the CMS and those having specialized CRMS skills;

c) Personnel trained to perform verification activities including internal management system or cybersecurity audits;

d) Contractor support personnel;

e) Organizational infrastructure as needed in the CRMS design;

f) Technology as needed in the CRMS design; and,

g) Financial resources as needed in the CRMS design.

2.3.2 Roles and Responsibilities

Company management demonstrates its commitment by defining roles and responsibilities.

i) Roles

ii) Allocating responsibilities and accountabilities

a) Accountabilities and authorities are defined, documented, and communicated

iii) Delegating authorities, to facilitate effective cybersecurity risk management

a) Personnel with management responsibility demonstrate their commitment to the continuous improvement of cybersecurity performance. Senior level management takes final responsibility for cybersecurity and the CRMS.

2.4 Master's Responsibility and Authority

The Company defines and documents the Master's responsibility with regard to the following responsibilities. (Adapted from ISM 5.1)

i) Implementing the security controls designated for use with cyber-enabled and cyber-physical systems in accordance with policy of the Company;

ii) Motivating the crew to observe that policy;

iii) Issuing appropriate orders and instructions in a clear and simple manner;

iv) Verifying that specified requirements are observed; and,

v) Periodically reviewing the Cybersecurity Risk Management System and reporting its satisfactory performance or its deficiencies to the shore-based management.

The Company confirms that the CRMS is operating on board the ship and communicates a statement emphasizing the Master's authority. The Company also establishes in the CRMS procedures that the Master has the overriding authority and the responsibility to make decisions with respect to personnel, system, ship or vessel security, safety and pollution prevention, and to request the Company's assistance as may be necessary. (Adapted from ISM 5.2)

2.5 Shipboard Personnel

2.5.1 Master

The Company confirms that the Master is (Adapted from ISM 6.1):

i) Fully conversant with Company's Cybersecurity Risk Management System, and

ii) Given the necessary support so that the Master's duties can be effectively performed in ensuring the CyberSafety of the ship, its systems, and its cyber-physical functions.

2.5.2   Crew

The Company confirms that the crew is appropriately trained for safety and security. (Adapted from ISM 6.2)

i)   The Company establishes procedures to confirm that new personnel and personnel transferred to new assignments related to cyber-physical systems, their safety and security, and protection of cyber-enabled systems that could affect the environment, are given proper familiarization with their duties. Instructions which are essential to be provided prior to sailing are identified, documented, and given. (Adapted from ISM 6.3)

ii)   The Company establishes procedures by which the ship's personnel receive relevant information on the Cybersecurity Risk Management System in a working language or languages understood by them. (Adapted from ISM 6.6)

iii)   The Company confirms that the ship's personnel can communicate effectively in the execution of their duties related to the Cybersecurity Risk Management System. (Adapted from ISM 6.7)

iv)   The Company confirms that persons in the workplace take responsibility for aspects of cybersecurity over which they have control, including adherence to the Company's applicable cybersecurity requirements.

2.6   Cybersecurity Risk Management System Documentation

CRMS documentation contains or references the following information as a best practice.

i)   CRMS design architecture diagram with a reference to each risk contributor identified in the risk management plan is resolved by each architecture feature.

ii)   Established, implemented, and cyber management documented procedures for:

   a)   Policy and procedural document and data control, including documents of external origin

   b)   Security or cybersecurity internal audits

   c)   Security-related corrective and preventive action

   d)   System non-conformances, declared incidents, hazardous occurrences, and near misses

   e)   Control of system testing and quality records

iii)   Documents describing a system or application test (quality) policy and cyber security testing objectives.

iv)   CRMS quality manual describing system testing.

v)   Documents required for effective planning, operation, and control of its cyber management processes.

vi)   Documentation demonstrating compliance with requirements and of effective operation of the management system. This documentation can be in any form or type.

2.7   Operational Control

2.7.1   Shipboard Cyber-related Operations

The Company establishes procedures, plans and instructions, including checklists as appropriate for key shore-based and shipboard cyber-related operations and activities concerning the safety of personnel, safety of the ship, prevention of pollution. The procedures also describe other activities that can be affected by software-intensive or cyber-physical systems in support of the Company policy(s), objectives, and action plans. The various tasks are defined and assigned to qualified personnel.

2.7.2 Flag State

The Company establishes, implements, and maintains documented instructions and procedures to promote cyber-safe operation of ships, offshore vessels and the associated shoreside facilities and protection of the environment in compliance with relevant international and flag State legislation.

2.7.3 Controlled Conditions

The Company identifies those operations and activities that are associated with identified hazards and significant cyber-enabled system risk areas where control measures need to be applied to manage the risk(s). Such controls include software management of change. The Company plans these operations and activities for implementation under controlled conditions. The output of this planning is in a form suitable for the Company's method of operations. Controlled conditions include the following information and verifications.

i)   Compliance with mandatory rules, regulations, and codes;

ii)   Established and maintained documented procedures/work instructions to control situations where their absence could lead to deviation from the policies, objectives, and targets;

iii)   Defined tasks assigned to properly qualified personnel;

iv)   The Company's permit to work system, which include measures to verify that the condition of spaces and systems as safe or not safe for work is readily identifiable. These measures are also to include safeguards so that work does not proceed unless safe conditions exist. The condition of spaces or systems being worked on is updated as appropriate throughout the course of the work;

v)   Supply chain controls related to purchased goods, equipment, and services;

vi)   Third party access controls related to contractors and other visitors to the workplace;

vii)   The availability of suitable monitoring and measuring equipment;

viii) Implementation of monitoring and measurement;

ix)   Validation of approved processes and equipment, as appropriate, and required records; and,

x)   Controls and procedures in place for OEM and vendor remote access to systems, sensors, data, or components that maintains ship personnel control over safety-critical systems.

1   ABS *(1 August 2023)*

ABS Rules for Building and Classing Marine Vessels

ABS Rules for Building and Classing Mobile Offshore Units

ABS *Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety*® *Volume 1*

ABS *Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafety*® *Volume 3*

ABS *Guide for Software Systems Verification – ABS CyberSafety*® *Volume 4*

ABS *Guidance Notes on Software Provider Conformity Program – ABS CyberSafety*® *Volume 5*

ABS *Guide for Cybersecurity Implementation for U.S. Government Vessels, Facilities and Assets – ABS CyberSafety*® *Volume 6*

ABS *Guide for ABS CyberSafety*® *for Equipment Manufacturers – ABS CyberSafety*® *Volume 7*

ABS *Guide for Dynamic Positioning Systems*

ABS *Guide for Software Quality Management (SQM)*

ABS *Guide for Risk-Based Inspection for Floating Offshore Installations*

ABS *Guide for Smart Functions for Marine Vessels and Offshore Units*

ABS *Guide for Surveys Based on Machinery Reliability and Maintenance Techniques*

ABS *Guidance Notes on Reliability-Centered Maintenance*

ABS *Guidance Notes on Risk Assessment Application for the Marine and Offshore Industries*

ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*

ABS *Guidance Notes on Smart Function Implementation*

2   IEEE

IEEE Std 14764-2006, Second edition 2006-09-01, Software Engineering – Software Life Cycle Processes – Maintenance

IEEE/ISO/IEC 12207-2017, Systems and Software Engineering – Software life cycle processes

IEEE Std 730-2002, IEEE Standard for Software Quality Assurance Plans

IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation

IEEE Std 1016-1998, IEEE Recommended Practice for Software Design Descriptions

IEEE Std 1219-1998, IEEE Standard for Software Maintenance

IEEE Std 1362-1998 (R2007), IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document

IEEE SWEBOK 2004, Software Engineering Body of Knowledge

3   IEC

IEC 61508-0 (2005-01), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508

IEC 61508-1 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

IEC 61508-2 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC 61508-3 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

IEC 61508-4 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

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

IEC 61508-6 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

IEC 61508-7 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures

IEC 61511-1 Ed. 2.1 (2017), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

IEC 61511-2 Ed. 2.0 (2016), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1

IEC 61511-3 Ed. 2.0 (2016), Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels

IEC 62351 (Power systems management and associated information exchange – Data and communications security)

ISA/IEC 62443 (Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the Information Security Forum (ISF))

4   ISO

ISO 17894-2005 General principles for the development and use of programmable electronic systems in marine applications

ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model

ISO 9001:2015, Quality Management Systems – Requirements

ISO/IEC 20000-1:2011 Information Technology – Service Management – Part 1: Service management system requirements

ISO/IEC 27001:2013 – Information Technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013 – Information Technology – Security techniques – Code of practice for information security controls

ISO 28001:2007 – Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and plans – Requirements and guidance

ISO 31000:2009 – Risk management – Principles and guidelines

ISO 45001:2018 – Occupational Health and Safety Management Systems

5   NIST

National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018.

NIST Special Publication (SP) 800-12 Rev.1, An Introduction to Information Security.

NIST SP800-30, Rev.1, Guide for Conducting Risk Assessments.

NIST SP800-37, Rev.2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and privacy.

NIST SP800-39, Managing Information Security Risk: Organization, Mission and Information System View.

NIST SP800-53, Rev.5, Security and Privacy Controls for Information Systems and Organizations.

NIST SP800-53A, Rev.4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.

NIST SP800-82, Rev.2, Guide to Industrial Control Systems (ICS) Security.

NIST SP800-128, Guide for Security-Focused Configuration Management of Information Systems.

NIST SP800-137, Information System Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

NIST SP800-160, Vols1-2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems.

NIST SP800-171, Rev.1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

NIST SP800-171A, Assessing Security Requirements for Controlled Unclassified Information.

6   Other

American Waterways Operators (AWO). Cyber Risk Management: Best Practices for the Towing Industry, Version 1.0, 2018.

Industry Working Group Guidelines (IWGG). *Guidelines on Cyber Security Onboard Ships, Volume 3*, 2018, produced by an industry working group comprised of BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL.

International Association of Classification Societies, #166, Recommendation on Cyber Resilience.

International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code).

International Ship and Port Facility Security Code (ISPS) framework.

NERC CIP Standards (North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP)) - Targeted at the energy sector.

Oil Companies International Marine Forum (OCIMF). Tanker Management and Self-Assessment edition 3 (TMSA3), 2017.

Software Engineering Institute. The Capability Maturity Model: Guidelines for Improving the Software Process, Reading, MA, Addison-Wesley, 1995.

United States Department of Energy, Cybersecurity Capability Maturity Model (C2M2) Program, 2014.