



GUIDE FOR

CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES

ABS CyberSafety™ VOLUME 2

SEPTEMBER 2016

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

**© 2016 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

In the maritime world, safety and security are closely linked. The mission of ABS is to serve the public interest as well as the needs of our members and clients by promoting the security of life and property, and preserving the natural environment. For over 150 years, ABS has devoted its energies to promoting safe and efficient commerce by sea through the development and application of industry consensus standards. Initially, the emphasis was on safety, and ABS applied its technology and knowledge to maintain safety through prevention of accidents caused by the forces of nature and human error. While the science of those causes is very complex and is continually being improved, they are amenable to analysis, understanding and prediction. Through the dedication and diligence of everyone in the maritime industries, the safety record of shipping has steadily improved through the years.

Cybersecurity introduces an additional element into the safety equation: security against deliberate actions intended to cause harm. Security has always been a concern with naval ships, and the military routinely exercise precautions to maintain the security of their ships and offshore assets. Commercial vessels routinely employ special security measures under certain circumstances to prevent theft, piracy, smuggling or stowaways. Those crimes are usually economically motivated, where destruction is not the goal. Acts of terror are usually politically motivated, and ships and offshore assets are prime targets because of their mobility and high potential for causing extensive damage to life, property, the environment, and the transportation and economic infrastructure. The maritime community has come to the realization that ships and offshore assets must be made less vulnerable to security threats, both at sea and while in port. Perpetrators of such acts have moved toward cyber-attacks for similar purposes. Exposure to these threats has become pervasive due to the exponential growth of automation methods – and increasingly, autonomy – that has penetrated nearly all aspects of shipboard and offshore asset systems. Because these systems control multiple aspects of asset, ship or platform operations, they become integral parts of system and operational safety.

ABS supports the marine and offshore communities by developing the standard for marine and offshore cybersecurity, developing new methods and leading industry with best practices in a commitment to safety and security of life and property and preservation of the environment.

Cybersecurity refers to the security of information networks and control systems and the equipment and systems that communicate, store and act on data. Cybersecurity encompasses systems, ships and offshore assets, but includes third parties – subcontractors, technicians, suppliers – and external components such as sensors and analytic systems that interface with networks and data systems. This includes human interaction of crews and other Company personnel, customers and potential threat players. In such a dynamic system, cybersecurity is an evolving set of capabilities inside the Company, developing and adapting as technology and threats evolve.

Volume 1 of the ABS CyberSafety™ series provides best practices as a foundational element of overall safety and security within and across the marine and offshore communities. Cybersecurity encompasses a number of elements including basic cyber systems operations, system and system of systems requirements to enhance safety as well as cyber security in the interest of enhanced safety. This document is Volume 2 of the ABS CyberSafety™ series. It provides criteria for the assessment of corporate systems and asset readiness to prevent cyber events that may compromise the safety and security of the data, systems and assets.

ABS offers the optional **CS** series (**CS1**, **CS2**, and **CS3**) Class notation to ships and offshore assets that comply with ABS requirements contained in this Guide. The notation is available for all classed vessels complying with the IMO International Safety Management (ISM) Code. While the notation is not required as a condition for ABS Class, ABS believes that the ABS CyberSafety™ Class notation is a useful indication of the due diligence applied by owners to better prepare for cybersecurity concerns affecting ships, offshore assets and their associated shoreside facilities.

The maritime cybersecurity area is evolving rapidly, and the International Maritime Organization (IMO), the International Association of Classification Societies (IACS), governmental authorities, and ABS are expected to add to the resources available to prepare Owners of ships and/or offshore assets for the new security environment.

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

ABS CyberSafety™ VOLUME 2

CONTENTS

SECTION 1	Introduction to the Guide.....	1
1	General	1
3	Application and Scope	1
3.1	Application	1
3.3	Scope	1
5	Certification	2
5.1	General.....	2
5.3	Certification Process.....	3
5.5	Survey and Certification Process.....	3
5.7	Representations.....	4
5.9	Termination.....	4
5.11	Limitation of Liability	4
7	Notation.....	5
9	Organizations	5
9.1	Company	5
9.3	Ship Builder Integrator (SBI).....	5
9.5	System Provider (SP)	5
9.7	Sub-Supplier (Component Providers)	5
11	Definitions	6
13	References.....	9
13.1	ABS	9
13.3	IEEE	10
13.5	IEC.....	10
13.7	ISO	11
13.9	Other.....	11
SECTION 2	The Cybersecurity Program	12
1	General	12
3	Process	12
3.1	Organizational Capabilities	13
3.3	Risk Assessment	13

3.5	Management Systems.....	14
3.7	Systems and Equipment.....	14

FIGURE 1	Categories of Capabilities within the ABS CyberSafety™ Model	13
----------	--	----

SECTION 3 Assessment of Cybersecurity Implementation for an Organization and its Assets..... 16

1	ABS CyberSafety™ Notation Implementation	16
3.1	Baseline – Limited Cybersecurity Awareness Implementation (Lowest level of Readiness)	16
3.3	CS1 – Informed Cybersecurity Implementation (Basic)	17
3.5	CS2 – Rigorous and Repeatable Cybersecurity Implementation (Developed).....	17
3.7	CS3 – Adaptive Cybersecurity Implementation (Highest level of Readiness) (Integrated).....	18
3.9	Applicability of Capabilities to Asset Protection	18
5	Applicability of Notations and Certifications.....	18
7	Safety of Personnel and Equipment	19
9	Onboard Testing	19
11	Capability Assessment Process	19
11.1	Company Decision Stages	20
11.3	Stage 1: Cybersecurity Assessment.....	20
11.5	Stage 2: CyberSafety Risk Assessment (CRA)	21
11.7	Stage 3: CyberSafety Management System Assessment (CMSA).....	21
11.9	Stage 4: CyberSafety Risk Profile Development (CRPD).....	21
11.11	Stage 5: CyberSafety Capability Assessment (CCA)	21
13	Functional Description Document (FDD) and Document Submission Requirements	21

FIGURE 1	Cybersecurity Notation Hierarchy	16
----------	--	----

FIGURE 2	Capability Assessment Process.....	20
----------	------------------------------------	----

SECTION 4 Requirements for Certification..... 23

1	Categorization of Security Program.....	23
3	Requirements and Capabilities Required for ABS CyberSafety™ Notation/Certification.....	23
5	Specific Requirements and Capabilities for Operational Technology	24
7	Use of the Capability Matrix	24

FIGURE 1	Capability Sets in Relationship to One Another	25
----------	--	----

SECTION 5 ABS CyberSafety™ Capability Matrix..... 27

1	Capability Matrix	27
---	-------------------------	----

SECTION 6	Cybersecurity Management System	98
1	Management of CyberSafety	98
3	Planning	102
3.1	Cybersecurity Environment Aspects	102
3.3	Cybersecurity Implementation Planning	102
3.5	Cybersecurity Hazard Identification, Risk Assessment, and Risk Control	102
3.7	Legal and Other Requirements.....	103
3.9	CyberSafety Baseline	104
3.11	Management Programs	104
3.13	Cybersecurity Management System Documentation	105
5	Implementation and Operation.....	105
5.1	Resources, Roles, Responsibility, Accountability, and Authority	105
5.3	Master's Responsibility and Authority	106
5.5	Shipboard Personnel	106
5.7	Control of Documents	106
5.9	Operational Control.....	107
SECTION 7	Surveys After Construction and Maintenance of Class: ABS CyberSafety™ Requirements	108
1	General	108
3	Surveys for the ABS CyberSafety™ Notation.....	108
3.1	Survey Intervals and Maintenance Manuals/Records.....	108
3.3	Annual Surveys.....	108
3.5	Special Periodical Surveys	109
3.7	Facility Surveys.....	109
5	Modifications, Damage and Repairs	110
APPENDIX 1	Sample CyberSafety Management System Compliance (CMSC) Certificate	111
APPENDIX 2	Sample Certificate of Cyber Compliance (CCC) for the Company	112



SECTION 1 Introduction to the Guide

1 General

This Guide for ABS CyberSafety™ has been developed so as to reduce cybersecurity-related conditions or incidents that may negatively affect systems, ships, offshore assets, safety, or the performance of cyber-enabled systems. ABS recognizes the positive impact that sound cybersecurity management practices have in reducing losses to the maritime industry due to unauthorized access into control systems from criminal or unintended activity. This Guide provides a model for implementing cybersecurity programs.

This Guide presents criteria for compliance with ABS CyberSafety™ requirements. These requirements will be used by ABS in the cybersecurity reviews and surveys of information technology (IT) systems; operational technology (OT) control systems; and their system interfaces and software on ships, offshore assets and the management systems of the associated shoreside facilities.

This Guide emphasizes implementation and verification of organizational processes and business rules (i.e., controls) through review and audit methods, and technical verification of system protective mechanisms and technical controls through system testing.

Criteria for the hardware and software integrity of computer-based control systems are given in other ABS Rules and Guides, such as the *ABS Rules for Building and Classing Steel Vessels (Steel Vessel Rules)*, the *ABS Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*, the *ABS Guide for Integrated Software Quality Management (ISQM)*, and other applicable national and international standards.

3 Application and Scope

3.1 Application

This Guide is intended for use by companies operating all types of ships and offshore assets. The Guide's requirements are stated in general terms in order to apply to a wide variety of ships and offshore assets and their operating Companies.

The term "ships" includes passenger ships, cargo ships, mobile offshore units, and high speed craft. This Guide may also be used for fixed or floating offshore production assets. If requested by the owner, ABS will verify and certify the Cybersecurity program of any ship or vessel and its associated shoreside facilities in accordance with this Guide.

In general, this Guide is intended to apply to vessels and their operating Company. A vessel may be certified without certifying the Company or its facilities so long as appropriate boundaries are defined and verified in accordance with this Guide.

3.3 Scope

The requirements herein are applicable to standalone or integrated computer-based information technology and operational technology systems. Such systems may be installed on a ship, offshore unit, or land based Company facilities.

Compliance with the procedures and criteria given in this Guide may result in issuance of a:

- CyberSafety Management System Certificate (CMSC) and Notation **CS1**, **CS2**, **CS3**, to an ABS classed ship or offshore asset upon request. Ships and offshore assets not classed by ABS can be issued a "Statement of Fact" when they are in conformance with the requirements of this Guide.
- Certificate of Cyber Compliance (CCC) for the Company's examined Facility;

The intent of the **CS** Notation series is to define boundaries of critical systems in the shipboard networked environment. Primary Essential Services, as defined by Integrity Levels and criticality to human, asset or environmental safety, are to be protected for a vessel or unit to be eligible for the **CS** notation, within the defined system boundaries. Primary Essential Services are defined in 4-8-1/Table 1 of the *Steel Vessel Rules* or 4-1-1/Table 3 of the *MODU Rules*.

Operational Technology (OT) in Primary Essential Services, including process and systems control hardware and software, is addressed in ABS CyberSafety™ with the intent that control systems are built and operated in known conditions; that without operator alerts they cannot be accidentally or malevolently affected in ways that impact human, system or environmental safety; and that OT is sustained and maintained across its lifecycle with proper care and diligent attention to keep both controls and their systems safe.

Additional functions of the connected equipment are not included in the Notation unless detailed in the verification plan.

5 Certification

5.1 General

Companies seeking certification to this Guide must, as a condition of certification, conform to the requirements of the ISM Code as relevant to the selected scope of their organizational management system.

The scope of certification chosen by the Company may include vessels, offshore assets, and/or the Company's facilities in combination(s) chosen by the Company. Vessel selection considers all vessels in the fleet but centers on the vessels considered highest priority by the Company. At least one vessel of each selected type is to be presented as a sample to be maintained at certification within the same scope of certification as required by the Company. The Company must provide evidence of verifiable similarity¹ among ships and offshore assets of specific types if any survey or test operations are to be abbreviated on the basis of identical installations or commonality across ships and offshore assets.

Ships and offshore assets certified to the requirements of this Guide are, as a prerequisite, to be Classed by ABS or another International Association of Classification Societies (IACS) member to confirm CyberSafety builds on existing safe, monitored and managed assets. In the case of critical equipment or systems requested for specific review under the terms of this Guide, those systems must be Classed by ABS or another IACS member prior to consideration, for the same reasons as for ships and offshore assets Class requirements.

Vessels shall be assessed on an annual basis, when there are major cyber-enabled, safety-related networked system configuration changes², or with multi-year Class survey events when no major system configurations are changed. Annual Surveys are to be made within three months before or after each anniversary date of the crediting of the previous Special Periodical Survey or original construction date. Surveys/Audits for Certification to this Guide will be harmonized with extant ABS Classification, Statutory and HQSE-En survey/audit cycles to the extent possible.

A Company's Facility that is assessed by ABS and found to meet the requirements specified in this Guide may be issued a corresponding Certificate of CyberSafety Compliance (CCC). Vessels operating under the Company's Cybersecurity Management System that are assessed by ABS and found to meet the requirements specified in this Guide may be issued a CyberSafety Management System Certificate (CMSC) as findings of the assessment, and corresponding private notation in the ABS *Record*³. The Notations and their meanings are listed below in Subsection 1/7.

All certificates are subject to periodic and intermediate verifications conducted at each certified location. All certifications are nontransferable. Assessments are based upon a sampling process. The absence of recorded nonconformities does not mean that none exist. Nothing contained herein or in any certificate, notation, or

¹ Similarity includes not just type design (unit 1, unit 2, of a series), but also similarity of control system construction and implementation. Programmable Logic Controllers (PLCs) used in specific systems must be shown as sufficiently similar across units with a ship type that understanding of control systems is possible through documentation of those systems.

² Examples of changes sufficient to force reassessment of cyber-enabled, safety-related networked systems include major-version-number operating system or firmware changes in either OT or IT; 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 also apply.

³ As stated in 1/3.3, non-ABS-classed vessels will be issued a Statement of Fact in place of the CMSC and Notation.

report issued in connection with a certificate and/or notation is intended to relieve any designer, builder, owner, manufacturer, seller, supplier, repairer, operator, insurer, or other entity of any duty to inspect or any other duty or warranty, express or implied, nor to create any interest, right, claim, or benefit in any insurer or other third party.

This Guide is subject to review and revision. Updates may include, among other things, additional requirements, or clarification of existing requirements. All Guide related modifications need to meet the latest version of the Guide and major changes may require the entire system be recertified to the latest version of the Guide. Survey requirements are to be carried out to the latest Guide, and we reserve the right to make any changes or updates retroactive.

5.3 Certification Process

Companies seeking certification to the requirements of this Guide shall fulfill the following responsibilities, some of which are more fully described in subsequent sections of the Guide:

- i) Document, implement, and maintain a cybersecurity management system in accordance with the pertinent requirements of this Guide.
- ii) Provide ABS copies of Cybersecurity Management System documentation for review, in accordance with the requirements of this Guide.
- iii) Allow ABS access to all certified locations and vessels during appropriately scheduled working hours so as to assess the Cybersecurity Management System and relevant systems (information technology (IT), operational technology (OT), or both, including data infrastructure and interface systems) to determine continuing compliance with the pertinent requirements of this Guide.
- iv) Maintain a log or compiled record of all modifications, maintenance and system security or configuration updates and upgrades, including any outstanding help desk tickets or vendor/integrator repair or maintenance requirements, and any insecurities or breaches, and the resolution thereof⁴.
- v) Notify ABS of port state detentions of vessel(s). In the case of cyber-enabled, safety-related system assessments, inspections or audits that result in unsatisfactory port state findings concerning systems included in the verification plan for this Notation, note to ABS the details of the same.
- vi) Inform ABS in writing when an ISM Document of Compliance (DOC) or Safety Management Certificate is withdrawn or invalidated by the issuing party for vessels certified to the requirements herein.
- vii) Submit plans and data as documented in Appendix 1 of this Guide.
- viii) Inform ABS in writing of major changes to organizational management system elements (e.g., managerial organizational structure, location, change in types of vessels operated, upgrade/downgrade of process capability, control, or flow) so that the changes may be evaluated by ABS and appropriate action taken.

5.5 Survey and Certification Process

- i) ABS CyberSafety™ certification is an annual process for ships and/or facilities that seek to achieve and maintain the Notation and/or certificate. Survey for ABS CyberSafety™ certification includes the factors listed in 1/5.3 above, emphasizing documentation, operational cybersecurity management system viability, strict control of configurations and changes in networked or cyber-enabled assets, and organizational capabilities in place and functioning. Detailed checklists, supplementing the capability specifications in Section 5, will be provided for progress checking and current-status documentation.
- ii) Periodicity for ABS CyberSafety™ certifications will harmonize with standard ABS Survey requirements, and ABS will coordinate surveys and evidence-based assessments wherever possible.

⁴ This log is to be in a digital, searchable form. Non-searchable images of system, ship or asset operational manuals in documentation packages extend the duration and difficulty of survey and assessment. Proprietary documentation will remain with the owner, builder, operator, etc. if so specified or desired.

- a) *Surveys During Construction.* ABS Engineering and Survey personnel assigned to a newbuild project will actively collaborate to check design such that safety principles are integrated, and that ABS CyberSafety™ assessments and survey(s) are conducted in consonance with conventional survey events.
 - b) *Surveys After Construction.* The regular survey process, including both Annual and Intermediate Surveys, will be supplemented by ABS CyberSafety™ assessments as required. Annual recertification includes the documentation required in 1/5.3 above, given the fluid nature of information and automation technologies.
 - c) *Special Surveys.* ABS CyberSafety™ surveys and assessments may be required after equipment or control system changes (major system changes or configuration changes), after security events occur, or on an as-required basis from the Company.
 - d) Certification will expire at the end of the stated period on the CCC or CMSC. Recertification, assuming documentation is provided (as in 1/5.3 above) and reassessment or testing is completed in a timely fashion, is expected to be a shorter and more streamlined evolution than initial certification.
- iii) *Relationship between Survey (or Continuous Survey) and ABS CyberSafety™ Certification.* Class, as maintained through regular Surveys or through Continuous Survey, reviews overall technical and procedural compliance for requirements in accordance with the overarching Steel Vessel Rules, outside the ABS CyberSafety™ certification. Class, especially in conditions of Continuous Survey, includes ABS CyberSafety™ certification when requested, though said certification is a snapshot in time within the Class continuum. Results of the ABS CyberSafety™ certification will affect Class only when/if safety-critical findings are found that are determined to compromise the safety of life, ship or asset, or the environment.

5.7 Representations

Certification is a representation by ABS that at the time of assessment the Company and vessels, as pertinent, has established and implemented a Cybersecurity Management System in accordance with the requirements in this Guide for the specified certificates and notations, and that the assessments, inspections, tests and audits for appropriate security profiles and risk conditions were completed satisfactorily. Certification is not a representation that the Company always acts in compliance with the cybersecurity program or that the cybersecurity program addresses all contingencies. Management performance remains the responsibility of the Company.

5.9 Termination

The continuance of certification or any notation is conditional upon the Company's and vessels' continued compliance with the pertinent requirements of this Guide. ABS reserves the right to reconsider, withhold, suspend, or cancel the certification or Notation for noncompliance with the Notation requirements, refusing access to a vessel, unit, or facility for an assessment or verification, or nonpayment of fees which are due on account of certification and other services.

Upon change of vessel or asset ownership, or of management organization, ABS reserves the right to perform out-of-cycle reassessments to check that the Notation remains current under the new organization. The essence of this Guide is building, maintaining and sustaining enabling capabilities for security and safety of cyber-enabled systems; a change in ownership or management will necessarily indicate a change in Company capability to support secure and effective operations in vessel or asset systems.

5.11 Limitation of Liability

ABS shall not be liable or responsible in any respect for any inaccuracy or omission in this Guide or any other publication or document issued by ABS related to this Guide. Every owner, builder, or operator must understand their systems in order to tailor the application of security controls and requirements, filling gaps in their security where needed by specific situations. This Guide is not meant to address every possible contingency, but rather provide a means by which owner/builder/operator may execute a security program that may, in operations, reveal needs for tailored or unique security controls.

7 Notation

The **CS** Notation will be assigned upon achieving compliance with the procedures and criteria given in this Guide for cybersecurity implementation and subsequent verification. Maintenance of the **CS** notation over the operational life of the vessel, platform, facility or asset is subject to continued compliance as evidenced by satisfactory completion of periodic surveys conducted onboard the vessel, or at the asset or facility. The intent of the Notation is to define boundaries of safety-critical systems in the shipboard or platform networked environment, (i.e., ABS CyberSafety™ verification will address systems critical to human, vessel, platform, system or environmental safety and will be detailed in a verification plan). Non-safety-related connected control systems or information systems and non-safety-related functions of the connected equipment are not included in the Notation unless detailed in the verification plan. The **CS** notation may be assigned as follows:

- CS1** Informed Cybersecurity Implementation
- CS2** Rigorous Cybersecurity Implementation
- CS3** Adaptive Cybersecurity Implementation (Highest level of Readiness)

CS1, **CS2**, or **CS3** are more fully described in Section 3 of this Guide. The **CS** notation will be made available to the owner via the ABS *Record* in a protected form enabling disclosure by the owner only to parties with a need to know⁵.

The **CS** Notation may itself be annotated in the case of a Company that certifies a facility or facilities in addition to vessel(s). The Notation would thereby reflect as **CS1+**, **CS2+**, or **CS3+**. This is expected in cases of advanced vessels that will link control systems between vessel and onload/offload facility to regulate cargo or hazardous operations through cyber-enabled systems.

9 Organizations

9.1 Company

The Company is the Organization that initiates the project and owns the information system and/or control system at the end of the project.

9.3 Ship Builder Integrator (SBI)

For new builds, the SBI is the shipyard. If no shipyard is involved, then the activities and requirements listed for the SBI are to be performed by the Owner.

9.5 System Provider (SP)

System Providers (SP) are suppliers that developed the software for the system under software verification test subject to system verification. If multiple systems are selected for system verification, then there may be multiple SPs. This may also include Original Equipment Manufacturer (OEM) for majority of hardware systems.

9.7 Sub-Supplier (Component Providers)

A sub-supplier is a supplier of connected equipment to the SP's control system and subject to integration portion of the verification testing.

⁵ An expanded notation of **CS1+**, **CS2+**, or **CS3+**, as noted in Section 3, addresses ship and Company facility.

11 Definitions

The definitions listed below are taken, or adapted from the ISM Code, ISO 9001:2015, ISO 14001:2015, ISO 50001:2011, and OHSAS 18001:2007.

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

Acceptable Risk. Risk that can be tolerated by the Company having regard to its legal obligations and its own OH&S policy.

Administration. The Government of the State whose flag the ship is entitled to fly.

Anniversary Date. The day and month of each year that corresponds to the date of expiry of the relevant document or certificate.

Audit. Systematic, independent, and documented process for obtaining “audit evidence” and evaluating it objectively to determine the extent to which “audit criteria” are fulfilled.

Auditor. Person with the competence to conduct an audit.

Boundaries. Physical or site limits and/or organizational limits defined by the Company. (ISO50001:2011)

CCC. A Certificate of Cyber Compliance, which may be issued to a Company that is assessed by ABS and found to meet the requirements specified in this Guide.

CMSC. Vessels operating under the Company’s cybersecurity management system that are assessed by ABS and found to meet the requirements specified in this Guide may be issued a Cyber Safety Certificate (CMSC), containing findings of the assessment, and upon request a corresponding private notation in the *ABS Record*.

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

Certification. Confirmation decision by ABS that the Company’s management system meets the applicable requirements of this ABS Guide.

Company. The Owner of the ship or any other organization or person, such as the manager or the bareboat charterer, who has assumed the responsibility for operation of the ship from the ship owner and who, on assuming such responsibility, has agreed to take over all duties and responsibilities imposed by the ISM Code and this Guide; Organization [ISO 9001:2015, ISO 14001:2015, ISO 50001:2011, and OHSAS 18001:2007]. For Government-owned vessels in non-commercial service, the Naval Administration is to be considered the Company.

Company Information Security Officer (CISO). The individual responsible for information systems, control systems and data security within the Company’s enterprise.

Continual Improvement. Recurring process of enhancing the management system in order to achieve improvements in overall performance.

Control System. Set of devices that manages, commands, directs or regulates the behavior of other devices or systems according to user inputs, settings or configurations.

Correction. Action to eliminate a detected non-conformity.

Corrective Action. Action to eliminate the cause of a detected nonconformity or other undesirable situation.

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

Cybersecurity Management System. An organizational tool for the identification, prioritization, execution and monitoring of the Company’s cybersecurity policies, processes and procedures

CyberSafety Management System Certificate (CMSC). Certificate of compliance provided for a vessel’s successful assessment of capabilities and practices required for CyberSafety under this Guide, complementing the Notation provided on the vessel’s *ABS Record*.

DOC. ISM Document of Compliance certificate

Document. Information and its supporting medium.

Documentation. Records and certificates that confirm that the ship is in compliance with applicable security requirements.

Energy. Electricity, fuels, steam, heat, compressed air, and other like media.

Environment. Surroundings in which a Company and its ships or offshore assets operate, including air, water, land, natural resources, flora, fauna, humans, and their interrelation.

Environmental Aspect. Element of a Company's activities or products or services that can interact with the environment.

Environmental Impact. Any change to the environment, whether adverse or beneficial, wholly or partially resulting from a Company's environmental aspects.

Environmental Objective. Overall environmental goal, consistent with the environmental policy, that a Company sets itself to achieve, and which is quantifiable where practicable.

Environmental Management System. Part of a Company's management system used to develop and implement its environmental policy and manage its environmental aspects

Environmental Performance. Measurable results of a Company's management of its environmental aspects.

Environmental Target. Detailed performance requirement that arises from the environmental objectives

Executive Management. Person(s) who directs or controls a Company at the highest level.

FDD – Functional Description Document. Revision-controlled document containing a description of the industrial control system (ICS) equipment and control systems in a form readily understandable by shipboard personnel who are (a) technically competent in shipboard operations, and are (b) 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.

Hazard Identification. Process of recognizing that a hazard exists and defining its characteristics.

ICS – Industrial Control System. Control system for industrial or machinery processes.

Information System. Automated system that enables Company and 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.

Incident. Work-related event(s) in which an injury or ill health (regardless of severity) or fatality occurred or could have occurred.

Integrity Level. Assessment grade for the importance of a system to safety or operations, based on the consequences of failure of the function, component or system; represents how important the function is to the operation of the overall system.

Internal Audit. Systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the Company are fulfilled

Interested Parties. Person or group, inside or outside the workplace, concerned with or affected by the performance of the Company.

ISM. International Management Code for the Safe Operation of Ships and for Pollution Prevention as adopted by the formal body that determines these safety rules.

Major Non-conformity. The deviation that poses a serious threat to the safety of personnel or the ship or a serious risk to the environment that requires immediate corrective action or the lack of effective and systematic implementation of the requirement of the Code.

Mission-Critical System. A cyber-enabled component or system installed in a ship, facility, mission system or asset (e.g., offshore platform) that is required to carry out functions necessary to the business purposes of the system or asset, and without which the ship, facility, mission system or asset would be greatly hindered.

Non-conformity. An observed situation where objective evidence indicates the non-fulfillment of a specified requirement.

Notation. Documentation in the *ABS Record* upon certification to recognize that the ABS classed vessel meets the applicable requirements of this Guide.

Objective. A goal stated in terms of the management system's performance, that the Company sets itself to achieve.

Objective Evidence. Quantitative or qualitative information, records, or statements of fact pertaining to safety or to the existence and implementation of a safety management system element, which is based on observation, measurement, or testing that can be verified.

Observation. Statement of fact made during a management audit and substantiated by objective evidence.

Occupational health and safety (OH&S) – conditions and factors that affect, or could affect, the health and safety of employees, temporary workers, contractor personnel, visitors, and any other person in the workplace.

OH&S Management System. Part of the Company's management system used to develop and implement its OH&S policy and manage its OH&S risks

Operational Technology. Automated systems, including hardware and software, that performs direct monitoring and/or control of physical devices, processes or events; superset of industrial control systems.

Performance. Measurable results of the Company's management of its impacts and/or risks and achievement of its objectives.

Policy. Overall intentions and direction of a Company related to its performance as formally expressed by the top management.

Preventive Action. An act to eliminate the cause of a potential non-conformity or other undesirable potential situations.

Prevention of Pollution. Use of processes, practices, techniques, materials, products, services, or energy to avoid, reduce, or control (separately or in combination) the creation, emission, or discharge of any type of pollutant or waste in order to reduce adverse environmental impacts.

Procedure. Specified way to carry out an activity or a process.

Record. Document stating results achieved or providing evidence of activities performed.

Remote Access. A method of gaining access to distant assets through network connections; 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 such as secure shell (SSH).

Requirement. A need or expectation stated, implied or obligatory

Risk. Combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury, ill health, or system or environmental impact that can be caused by the event or exposure(s).

Risk Assessment. Overall process of evaluating the risk(s), arising from a hazard(s), taking into account the adequacy of any existing controls, and deciding whether or not the risk(s) is acceptable.

Safety Aspect. Element of a Company's activities or services that represents an actual or potential risk to safety or personnel, or the ship, relating directly to the Integrity Level of a given system and its criticality to overall human and system safety.

Safety-Critical System. A cyber-enabled component or system installed in a ship, facility, mission system or asset (e.g., offshore platform) that is required to carry out mission-critical functions, and which, through failure or incomplete operation, may cause safety impacts to personnel, to the ship or asset, or to the environment.

Ship Security Assessment (SSA). A risk based analysis of security-related hazards or threats for each ship the Company operates.

Ship Security Officer (SSO). The individual on board each ship who is responsible for ensuring that the SSP is implemented at all times while the ship is underway and in port. The SSO also is responsible for ensuring that the SSP is maintained up-to-date and that the ship's crew are trained and familiar with their security related duties.

Ship Security Plan (SSP). A ship-specific document based on the SSA that identifies equipment, measures and procedures that are to be employed to maintain security on board the ship.

Significant Energy Use. Energy use accounting for substantial energy consumption and/or offering considerable potential for energy performance improvement.

SMC. ISM Safety Management Certificate.

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

Supplier. Company or person that provides a product or service.

System. A set of interrelated or interacting elements required to direct and control a Company.

Two-factor authentication. Means of gaining access to resources with both personal login identifier and a technical factor (such as a changing-key fob or a mobile phone keycode) that confirms the identity of the user logging into the resource, and which helps to prevent illicit access by credential theft alone.

Work Environment. Set of conditions or physical location, under control of the Company, in which the work and related activities are performed.

In this document, text that appears in italics is taken directly from the cited standard. Text in standard font comprises the ABS recommendations and requirements.

13 References

13.1 ABS

ABS Rules for Building and Classing Steel Vessels

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 Dynamic Positioning Systems

ABS Guide for Integrated Software Quality Management (ISQM)

ABS Guide for Risk Evaluations for the Classification of Marine Related Facilities

ABS Guide for Survey Based on Reliability Centered Maintenance

ABS Guide for Surveys Using Risk-Based Inspection for the Offshore Industry

ABS Guidance Notes on Reliability-Centered Maintenance

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

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

ABS Guide for Surveys Based on Machinery Reliability and Maintenance Techniques

13.3 IEEE

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

IEEE Std 12207-2008, Second edition, 2008-02-01, 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

13.5 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 (2003-01), 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 (2003-07), 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 (2003-03), 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))

13.7 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

13.9 Other

ANSI/ISA-84.00.01-2004, Part 2 (IEC 61511-2 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative

National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Feb 2014.

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

American Petroleum Institution (API) Specification 16D Third Edition Draft: Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment. October 2014

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

International Ship and Port Facility Security Code (ISPS) framework



SECTION 2 The Cybersecurity Program

1 General

Cybersecurity is the application of security methods and controls to provide for, and to verify, deterministic behavior of cyber-enabled systems. A cybersecurity program is meant to safeguard assets, guide personnel and their actions, and allow freedom of action and of decision making within the boundaries of the system, free of interference from both internal and external influences. The cybersecurity process has a beginning but has no practical end short of decommissioning of the cyber-enabled asset.

Ship and offshore asset owners, operators and crew must understand their systems in order to use and protect systems, data, and asset functions. Poor cybersecurity can lead to loss of data or intellectual property; to loss of system integrity in both business-essential and business/mission/safety-critical systems; and to loss of system function in the critical control systems used to execute business processes. Cybersecurity can prevent losses when systems are designed, architected, engineered, built and operated with appropriate due care and due diligence.

Cybersecurity for systems must naturally provide security for people, data, systems and assets. Security for people must include periodic awareness training, systems training, and security policies and procedures. Security for assets includes the physical (ships, offshore assets, associated shoreside facilities and equipment) as well as the virtual (business data, process information, and intellectual property). But an organization's assets may also include its functions – those operations which keep the Company moving on its trajectory, which keep materiel flowing across production systems, or perhaps which keep raw materials moving through pipelines. Those functions that make the business viable are assets for the operation of the Company.

Systems that control production or operational systems, called operational technology (OT), are cyber-physical systems (CPS) that control processes and systems. These OTs or CPSs will have relevance to safety in their environments because they control direct physical effects in connected systems. They will often communicate with information technology (IT) general-purpose networks to provide sensor or operational data to management personnel. Because of the implications for CPS with safety consequences being connected to IT systems of differing trust levels, owners and operators require standards to which they can build and measure cybersecurity.

3 Process

The Company is responsible for setting the cybersecurity policies for the systems and ships/offshore assets it operates. As a minimum those policies must conform to international and domestic requirements, but they will also reflect the Company's objectives in maintaining safety and security onboard its vessels wherever they operate. The elements of a cybersecurity program include the following as minimum elements:

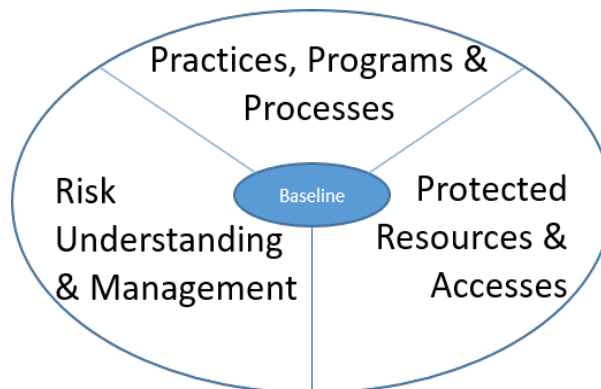
- Organizational capabilities suitable for defense from cyber threats;
- Risk assessment of cyber threats;
- Management system scope and depth suitable for defense from cyber threats; and
- System and equipment design and engineering to minimize cyber vulnerabilities.

ABS CyberSafety™ was developed to address these needs.

3.1 Organizational Capabilities

The ABS CyberSafety™ program is used to manage and measure levels of cybersecurity development, building organizational competence in defined capability areas. The capability areas encompass people, systems, processes and data, and form the core of organizational functions which implement the tasks and instantiate security controls. Organizational capabilities can be categorized into three related but distinct groups that describe the practices, programs and processes in a complete cybersecurity program. This is summarized in Section 2, Figure 1 below and more fully described in the *ABS Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety™ Volume 1*.

FIGURE 1
Categories of Capabilities within the ABS CyberSafety™ Model



Within the ABS CyberSafety™ model categories are the capabilities needed to achieve a measurable level of cybersecurity and CyberSafety. A capability is a functional approach to implementing a particular task set, combining people, systems, data and processes in order to execute a course of action in that capability area. Certain capabilities are required as a fundamental core to confirm the Company is prepared to move forward; these are the Baseline, noted above. Capabilities are built as the Company matures and brings more people, systems, data and processes into its operational environment.

3.3 Risk Assessment

Risk is the interplay among potential threats, Company assets, system vulnerabilities, impacts of incidents, and consequences of those incidents. The Guide requires and encourages understanding of risk conditions as part of the Basic Capability set (CS1), and as the Company expands and matures its cybersecurity program, this effort becomes risk management in the Developed Capability set (CS2).

A risk-based approach to cybersecurity in pursuit of CyberSafety entails the understanding of risk factors or risk conditions, with the business- or mission-based grasp of assets under risk. This allows prioritization of risk mitigation efforts, and it will guide the Company in building its security capabilities, implementing its security measures, and monitoring its security systems.

The Company must understand the value of its data and its intellectual property, and the value of its functional capabilities as enabled by cyber-physical systems. If control systems did not function correctly, and production machinery or processes ceased, the effect on the Company may be strong, no matter the source of the interference or interruption. Thus system function is considered an asset when working with control systems and operational technologies, especially in conjunction with cyber-enabled, safety-critical systems.

Assets may also include positive incentives as motivation for building capabilities, managing risks, and handling security. Data held in certain regulatory regimes, such as protected health information (PHI) or personally identifiable information (PII), or third-party data held by the Company, necessarily help the Company develop the prioritization of protections, tools and personnel assigned to protect those assets with Company systems. The Company's cybersecurity strategy, when based on risk assessment and risk understanding, will guide resource allocation in prioritization of tasks and capability development. When the most significant risk conditions or threat factors are used to develop and implement priority security controls, the Company is using a risk-based approach that can be measured and monitored.

3.5 Management Systems

The Company's Cybersecurity Management System is to address cyber security concerns and be subject to audit. Section 6 of this document defines the management system requirements for cybersecurity.

3.7 Systems and Equipment

3.7.1 Operational Technology

Operational Technology (OT) has been increasing in complexity and prominence for the last 30 years. Confusion resulting from blanket application of Information Technology (IT) management principles to an OT system is not only sub-optimal, but may very well be hazardous. Complex OT systems must be conceived, maintained, and tested quite differently than traditional IT networks and systems.

Increasingly OT systems are being connected to conventional (non-engineering) networks for monitoring, remote access or convenience. This exposes the OT systems to outside connectivity, potentially revealing vulnerabilities that could affect cyber-physical system operations.

The way forward relies on an understanding of the differences between OT-specific maritime cybersecurity and IT practices and appropriate handling. Policies and procedures must comprehend the differences in managing an OT network or system vs traditional IT methods.

3.7.2 Equipment Classification by Integrity Level and Potential Safety Impact

The judgment as to Integrity Level (IL) for safety-critical or safety-relevant systems will be considered in ABS CyberSafety™ assessments. Systems with direct safety impact within their systems, or secondary systems that could bring about potential failures in safety-critical systems, will be considered as requiring higher integrity levels than others that do not possess such features or functions. IL classification is in accordance with the *ABS Guide for Integrated Software Quality Management (ISQM)* and is represented as follows:

IL	Potential Consequences			Examples, not inclusive
	Safety	Environmental	Functional	
0	Negligible	Negligible	Minor impact on operation. Might affect supporting process system but not main process system	Entertainment System, Administrative computer systems, office network, Data Collection system (non-Authority required)
1	Might eventually lead to marginal safety incident	Might eventually lead to a marginal environmental incident	Might lead to maintenance shutdown of non-critical system. Main process continues to operate.	Non-essential control of systems, BPCS, Non-essential communication systems, Vessel Management System. New or unproven non-essential technologies minimum rating.
2	Within a short time could cause critical injury, lost time, accident or loss of a life.	Critical environmental impact	Shutdown of main system, excessive time for repair.	Drilling control system, BPCS, Safety Instrumented Systems (SIS) (minimum rating), PMS, essential systems, DP control system, main engine control system, safety systems, cargo control system, navigation system, new or unproven essential technologies minimum rating.
3	Immediate and Catastrophic lost time injuries, or multiple loss of life.	Catastrophic environmental impact	Significant repair time or loss of the marine or offshore asset.	Drilling Blowout Preventer control system, SIS or safety control systems, boiler firing control system, etc.

3.7.2 Security for All Components

Cybersecurity is generally focused on securing networks and devices on those networks. But other components must be included for defensibility and correct operations also. Transmission systems and lines must be safeguarded, whether by the Company or through its contracts with providers. Personnel must be trained for cyber-enabled system safety, resistance to criminal attack methods, and protection of organizational assets and critical systems or functions.

Resilience of critical systems is part of the cybersecurity implementation process. The result of resilience is that attacks or failures do not persist after incident response controls are executed and system restoration begun.

Defense in depth, the use of multiple means to view, protect and monitor networked assets, is an important part of resilience, as are architected solutions for designed-in resistance to unauthorized access or use; backup capabilities, such as redundant power or communications; user process definition as means to minimize errors or incorrect use; and system data restoration. Component security, with such features, helps confirm secure operational characteristics and integration with other systems in ways that do not introduce unexpected risks to the other systems. All these factors derive from the process and technology specifications in the Guide, combined with owner or operator insights or the assets protected.

3.7.3 Security and Remote Accessibility

Connections, communications and access to Internet Protocol (IP)-enabled sensors and systems that are considered components of the Internet of Things (IoT) or Industrial Internet of Things (IIoT) must be specifically addressed as part of the Operational Technology security measures onboard any ship, asset or facility. Remote accessibility to IoT/IIoT devices, especially, must be controlled carefully, as these devices are expected to be standalone, sealed, never-updated network participants, meaning that they can become conduits into primary networks if left exposed to unauthorized communications. These devices and similar systems are addressed in the OT specification in Section 5, with specific coverage under CS2's Capability 17.

Cloud storage and application providers also fall into the category for remote access. Authorized procedures for application and storage access must govern all communications with these offboard resources. Because of the nature of cloud communications, the primary protective requirements are human procedures and processes (such use of access control lists match against asset usage), with technical controls that specifically identify the user (two-factor or multi-factor authentication) when in contact with sensitive information systems or assets.

3.7.3 Management of Change for All Components

Notations in the **CS** series are dependent on owner/operator exercise of the capabilities as provided in the Guide, in addition to those capabilities and needs required by due diligence responsibilities, including management of change⁶. When a ship or asset is certified according to CS, ABS is to be notified when major changes are made to configurations or systems; when new interfaces between IT and OT are implemented, or existing interfaces are changed; or when new remote access methods are implemented for either IT or OT. ABS will communicate with the ship or asset management/owner, and with both IT and OT points of contact in these matters to confirm complete communications and understanding of changes and configurations.

⁶ The ABS Guide for Integrated Software Quality Management (ISQM) provides additional guidance on Management of Change processes.



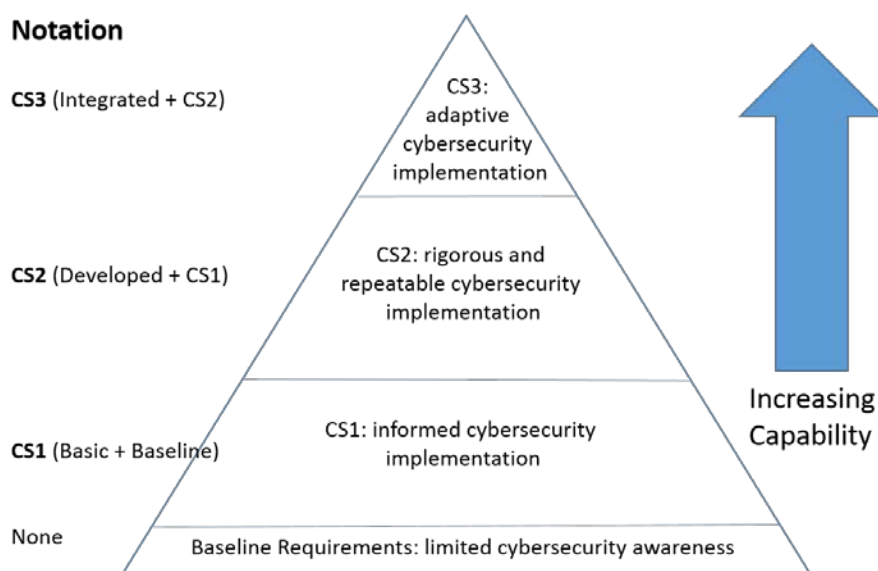
SECTION 3 Assessment of Cybersecurity Implementation for an Organization and its Assets

1 ABS CyberSafety™ Notation Implementation

This Guide differentiates organizations on two levels: first is the Company's implementation level or maturity, defined by the Notation assigned, and on the other level is the degree of implementation of the capabilities. Notations and capabilities combine as laid out below; capability implementation is the method the Company will use to move from one CS capability to another as it matures.

The ABS CyberSafety™ Notations provide context on how a Company views cybersecurity risk and the processes implemented to manage that risk, for either IT and/or OT. The Notations provide a method for gauging the relative thoroughness and rigor applied to cybersecurity risk management practices within the Company. It also provides the foundation by which ABS determines the robustness of the Company's cybersecurity protection and privacy protection programs. Section 3, Figure 1 below depicts the hierarchy of Notations:

FIGURE 1
Cybersecurity Notation Hierarchy



3.1 Baseline – Limited Cybersecurity Awareness Implementation (Lowest level of Readiness)

3.1.1 Risk Management Process and Process Documentation

The Company's IT and/or OT cybersecurity risk management practices are not formalized in the Company or aboard the asset, and risk is managed in an informal, reactive manner. Prioritization of cybersecurity and privacy protection may not be documented or based upon stated organizational risk objectives, the threat environment, business requirements, or the mission statement of the Company.

3.1.2 Formal Risk Management Program

The Company demonstrates limited awareness of cybersecurity risks at all levels of the Company, and a formal program for managing IT and/or OT cybersecurity risk is not evident. The Company's recognition and management of cybersecurity risks are guided by specific security incidents, and the response to those incidents is informed by external resources or internal resources that are not guided by job descriptions containing specialized cybersecurity knowledge. The Company does not have a permanent function implemented for managing cybersecurity incidents or communicating cybersecurity information within the Company.

3.1.3 External Participation

The Company has no formal process for coordinating, documenting or collaborating with external entities (e.g., other industry enterprises, international, federal, regional, and state authorities, class and certification bodies, etc.). This is important for IT, but it is a vital aspect of OT management and operations.

3.3 CS1 – Informed Cybersecurity Implementation (Basic)**3.3.1 Risk Management Process and Process Documentation**

The Company's risk management practices are approved by internal management, but those practices are not communicated in a formal IT and/or OT cybersecurity policy document. The Company's prioritization of cybersecurity activities is evidenced by informed employees who are in turn authorized and responsible for stating and managing documented organizational risk objectives, general and industry-specific threat environments, business/mission cybersecurity requirements, and cybersecurity regulatory imperatives.

3.3.2 Formal Risk Management Program

The Company documents and demonstrates an operational/organizational commitment to IT and/or OT cybersecurity within the Company. Risk-informed, management-approved ad hoc processes and procedures are defined and implemented, and staff has adequate resources to perform IT and/or OT cybersecurity duties. However, adherence to a documented cybersecurity reference model or framework is not evident. Cybersecurity information is informally shared within the Company.

3.3.3 External Participation

The Company can articulate its role in supporting or maintaining its' role in the maritime ecosystem, but has not formalized or documented its intention or capability for interacting with and sharing IT and/or OT cybersecurity information externally.

3.5 CS2 – Rigorous and Repeatable Cybersecurity Implementation (Developed)**3.5.1 Risk Management Process and Process Documentation**

The Company's IT and/or OT risk management practices are formally approved and expressed as policies and procedures. OT cybersecurity practices are regularly updated based on the application of risk management processes, changes in business/mission requirements, and changes to the threat and technology landscape.

3.5.2 Formal Integrated Risk Management Program

The Company demonstrates and documents an organization-wide approach to managing IT and/or OT cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, internally verified, and routinely reviewed. Formal organizations and consistent, repeatable methods are in place to respond effectively to changes in risk. Cybersecurity risk management activities are documented for review by internal and external assessment organizations. Cybersecurity activities are resourced, and responsible personnel possess the knowledge and skills to perform their appointed IT and/or OT protection roles and responsibilities.

3.5.3 External Participation

The Company understands its dependency upon informed agencies and partners, and receives information from these agencies and partners that enables collaboration and informed risk-based management decisions within the Company to respond to OT cybersecurity events.

3.7 CS3 – Adaptive Cybersecurity Implementation (Highest level of Readiness) (Integrated)

3.7.1 Risk Management Process and Process Documentation

The Company adapts its IT and/or OT cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the Company actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

3.7.2 Formal Integrated Risk Management Program

There is a Company-wide approach to managing cybersecurity risk that uses formal documented risk-informed policies, processes, and procedures to address potential cybersecurity events. Formal OT cybersecurity risk management organizational functions and general organizational awareness are demonstrably part of the organizational culture as derived from an awareness of embedded activities, information shared by other sources, and continuous awareness of activities on the Company's internal and linked systems and networks.

3.7.3 External Participation

The Company maintains internal expertise on IT and/or OT cybersecurity concerns, manages risks based on cybersecurity data and acquired intelligence, and actively shares information with partners to confirm that accurate, current information is being distributed and consumed to improve cybersecurity before an IT and/or OT cybersecurity event occurs.

3.9 Applicability of Capabilities to Asset Protection

Organizational capabilities give sustainability to the security protections, methods, systems and controls put into place to protect the Company's assets. Protected systems are mapped by the Company into the capabilities as they are operationally provided in the chosen levels (CS1-CS3) to run the Company, business, mission, etc.

Protected operational technology and information technology assets are directly connected to the requirements set forth as part of each capability specification. Potential failure modes and potential threats are to be considered within the context of each Company's environment, and as well within the context of the systems' installation environments⁷.

Organizational capabilities provide supportable, maintainable means to provide security and soundness of operations over time. The emphasis in building the capability levels for Notation is to provide the Company a sustainable program for security in multiple aspects (i.e., using many capabilities for holistic security) that allows deliberate decisions about resource allocation, relative risk and protective controls. The capabilities within a Notation may not be the only capabilities required to protect organizational assets. Further capabilities may be prudently chosen to complement a Notation in order to tailor Company resources and effort to its relative risk, given its assets⁸.

5 Applicability of Notations and Certifications

- i) ABS Class Notation for a ship or offshore asset, as applicable, will indicate **CS1**, **CS2**, or **CS3** based on protections and Company capabilities to support those protections for minimum sufficient security of the asset. The Notation will indicate **CS1+**, **CS2+**, or **CS3+** if the Company has an ABS Cyber Certificate (i.e., the Company has undergone ABS CyberSafety™ assessment for its related facility/facilities as well).

⁷ Operator errors can contribute to system failures, and the designed installation environment may alleviate some potential errors by removal of failure modes.

⁸ For example, a Company may certify a ship at CS1 (capabilities 1-9), but Company leadership may decide that implementing capabilities 16 (data security) and 17 (operational technology protection) is prudent for their relative risk position. The intent of the severable capabilities is to allow choices for flexibility and consistency in accord with organizational environment and situation, rather than to satisfy a particular stated list of tasks.

- ii) The CyberSafety Management System Certificate (CMSC), to be provided with the Notation, will list those systems, equipment, networks and interfaces assessed for the Notation. The CMSC will denote the current status of the ship or system(s), indicate any areas for continued attention, and the periodicity requirement for next inspection or assessment.
- iii) The Certificate of CyberSafety Compliance (CCC), provided to a Company for assessed facilities, will provide similar scope and content as CMSC, but tailored to the facility under assessment.

Additional scope of a Notation beyond specified Notation requirements, in the event of capabilities required by circumstance above a particular level of Notation, will be recorded in comments and verification plan for the Notation. Additional assets, such as Well Control, will be handled on a case-by-case basis.

7 Safety of Personnel and Equipment

Safety of personnel and equipment are to be considered by the Company and the Surveyor reflected in:

- i) The cybersecurity assessment and test plans, equipment setup, and other activities at the testing location (at factory or onboard) for safety of personnel and protection of equipment and the environment during execution of the Cybersecurity Assessment.
- ii) The re-activation of the system(s), from testing state to normal, controlling equipment for safety of personnel, equipment, and the environment.

Tests deemed to violate 3/7i) or 3/7ii) are either to have risk mitigated or the test is not to be performed.

9 Onboard Testing

While the control system is installed onboard and testing is to be performed, the Owner, SBI, and Verification and Validation (V&V) personnel are to agree on the functions or functionality to be tested and the safe method to perform the testing.

Tests or scenarios identified as having risk to safety, environmental, or equipment impacts damage are not to be tested onboard.

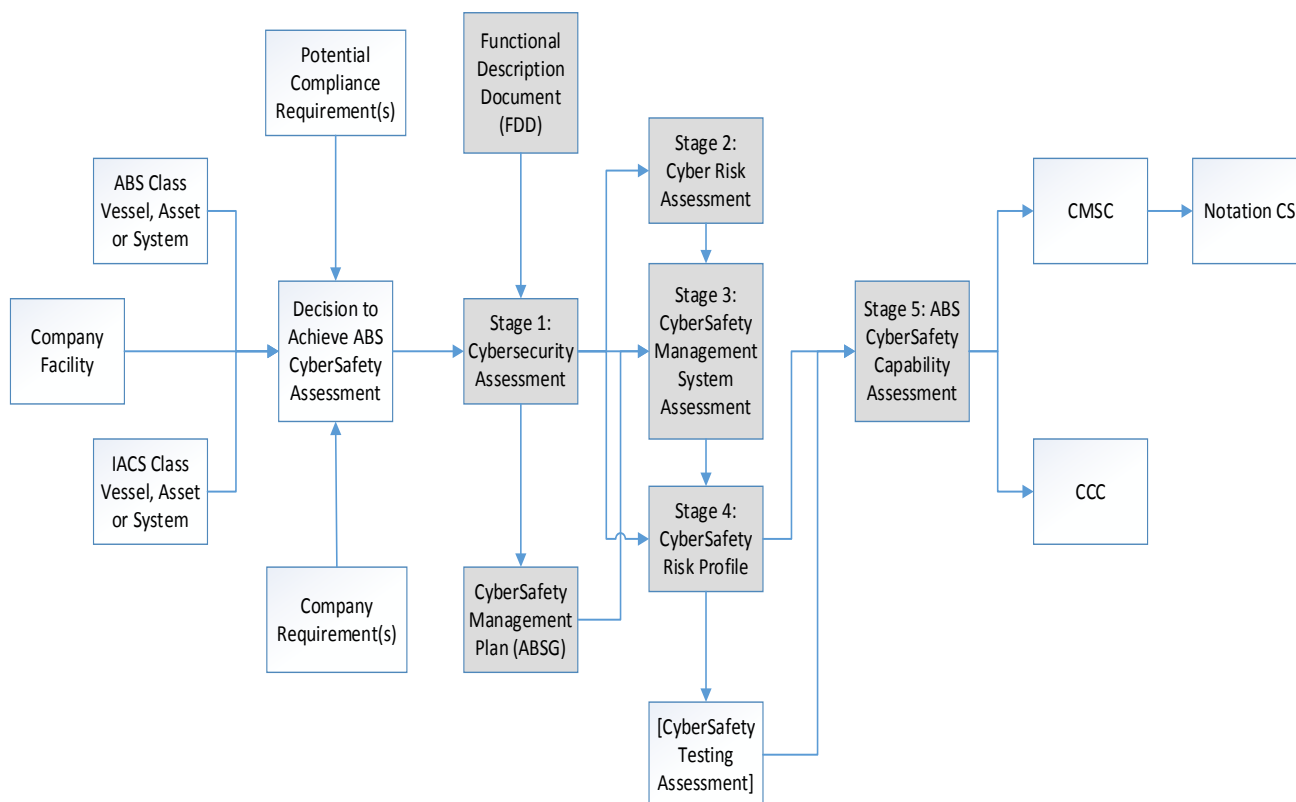
The Surveyor is to observe onboard testing and testing results as identified by test plans and scenarios. The Surveyor will not participate in any other role during testing.

11 Capability Assessment Process

The assessment process requires development of a stage-wise risk profile for the ship, asset or facility, following the engagement path shown in Section 3, Figure 2 below.

An initial ship or asset assessment will be a multi-part event that may be conducted in one contiguous time period, if ship or asset personnel and documentation are available, or it may be broken into parts to better match Company needs. Each stage will encompass specific objectives and will deliver products particular to those objectives. The expected outcome of the entire process is a capability assessment that shows any remaining gaps or decisions required to satisfy the Company's cyber-enabled systems safety and security requirements, along with the appropriate certificate and/or Notation when the process is complete to ABS and Company satisfaction.

FIGURE 2
Capability Assessment Process



11.1 Company Decision Stages

The left side (unshaded) of Section 3, Figure 2 shows several portions of the decision process that leads to the ABS CyberSafety™ certification. The Company decides what assets, vessels or facilities will be addressed in certification. Potential compliance requirements that may modify assessment needs, along with Company requirements for cybersecurity⁹, will contribute to this decision to pursue the certification process.

11.3 Stage 1: Cybersecurity Assessment

The initial Cybersecurity Assessment includes asset enumeration, policies and procedures examination, architectural documentation examination, and asset comparison with the Functional Description Document (FDD).

11.3.1 Functional Description Document

The FDD is the combined documentation associated with architecture, operations, security and testing of the mission-critical or business-critical systems aboard a ship, on an offshore asset, or in a facility. The expected content of an FDD is provided in Subsection 3/13 below.

11.3.2 CyberSafety Management Plan (CSMP)

The CSMP is a mid-way stage to establish a CyberSafety Management System (CSMS) if the Company does not have a method set in place to manage its critical systems' cybersecurity and safety postures. The CSMP is a work breakdown structure (WBS)-oriented program to develop and implement a capabilities-based CyberSafety program.

⁹ Internal requirements may flow from security or technology strategy, policies in place, or other expectations that the Company decides to include in the process.

11.5 Stage 2: CyberSafety Risk Assessment (CRA)

Stage 2 includes asset risk condition assessment, with a functional protective measures comparison against Company requirements. Threat matching with the protective measures will reveal any gaps the Company may have. The stage provides an Initial Risk Profile at conclusion.

11.7 Stage 3: CyberSafety Management System Assessment (CMSA)

Stage 3 assesses the Company's cybersecurity management across the organization and its assets, including automation methods, asset management and comparisons with the FDD, and cyber-related systems management and reporting. This stage provides templates and tools, as required.

11.9 Stage 4: CyberSafety Risk Profile Development (CRPD)

Stage 4 compiles all management system, asset assessments and risk assessment outputs to develop the Company Risk Profile. This uses the risk progression developed through previous stages to provide a measurable achievement profile for continued progress toward capability set certification.

11.11 Stage 5: CyberSafety Capability Assessment (CCA)

The CCA includes capability assessment, FDD assessment, interfacing systems assessment, networked systems audit, data integrity assessment and final certification for either CCC or CMSC and Notation.

13 Functional Description Document (FDD) and Document Submission Requirements

To support proper review in ABS CyberSafety™ assessments, the following documents are to be available to ABS for review. These documents comprise the Functional Description Document (FDD) in a constructive form, and they provide the visibility and understanding required for system assessment.

Documents and named artifacts include many such as the following:

- Integrity level reviews
- Safety Instrumented Systems (SIS) functions and status
- Failure Mode, Effects and Criticality Analysis (FMECA) records and updates (upon major configuration changes)
- Test reports and documentation, with retests
- Data logs from control systems
- Operations and Maintenance (O&M) Plan
- Control Equipment Registry
- Software Registry
- Software Management of Change (SMoC) Plan, Policy and Process
- Software Change Management Plan (CM)
- Software Configuration Management Plan, Policy and Process

Other documents commonly contain valuable data supporting documented processes and operational test results. Documents containing the following data are also to be available:

- Conditional states
- Integrity levels of components/systems
- Production system interfaces
- Human-Machine Interface (HMI) instructions
- Software versions, firmware, hardware by spec

- Constraints on system operations, with reasons
- All other interfaces (non-HMI, Supervisory Control and Data Acquisition (SCADA), data collection, with protocols and constraints)
- System conflicts and unresolved software issues
- Hardware and software obsolescence plans
- Reliability, Availability, Maintainability and Supportability (RAM-S) reviews
- Safety reviews



SECTION 4 Requirements for Certification

1 Categorization of Security Program

Security programs fall into the following general categories:

- *New Construction Asset.* New development of a security program with a new asset (marine, offshore or interfacing facility) in accordance with the owning Company's security and other guidelines and requirements.
- *New System.* Development of security for a new system, application or appliance, to be incorporated or integrated into an asset (marine or offshore) security program with either an existing or a new security program in effect.
- *Legacy Asset.* Existing system of system (ship, offshore platform, or other maritime asset with multiple existing standalone and networked systems) upon which a security program must be overlaid in accordance with organizational security and governance needs.
- *Legacy System.* Existing system for functional contribution to a legacy asset, new construction asset, or an interfacing facility, which may be networked or standalone.

3 Requirements and Capabilities Required for ABS CyberSafety™ Notation/Certification

A Company will build and provide capabilities to enable security in the Company. These capabilities provide continuous support for the security facets appropriate to the Company's security strategy. Assessment by ABS measures the scope and depth of those capabilities. An organization under assessment for CS1 (Basic), CS2 (Developed), or CS3 (Integrated) level certification is to demonstrate that:

- i) The Baseline requirements are met as a foundation for building Company capabilities for supportable, understandable and measurable cybersecurity;
- ii) The capabilities included in the level for certification are provided, supported and maintained by the Company;
- iii) The Company has tailored any further capabilities required – even if they are not part of the certification process in consideration – to confirm completeness of security;
- iv) The capability and its related specifications for Operational Technology have been considered and applied where appropriate for the process control and OT aspects of its architecture that have contact with, or impact upon, human safety-related conditions; and
- v) The security specifications, conditions and controls applicable under specific capabilities are implemented and monitorable/monitored as required to maintain security appropriate to the risk conditions understood in the Company.

The capabilities in all Sets bring rules with them, and it is important to understand that building and sustaining capabilities will require governance guidelines for consistent maintenance.

- Prioritization of security efforts across an Company can be accomplished with the levels provided in this Guide. Security for any particular organization must be tailored to its individual conditions, assets to be protected, risk conditions, and security threats. An implementing Company may choose to certify at Basic level, while needing to provide security from capabilities in the Developed level as well.

- Capabilities determine effective application of security controls and techniques. Capabilities determine effectiveness and sustainability of security measures in place in any Company's environment.
- A Company with a given level of certification, but with assets or operational needs in excess of that level, may require policy statements to guide their employees and system users that exceed minimum requirements for their certification level.

Assessment and grading a Company entails a two-fold evaluation, including security measures in place, and the Company's ability to support, sustain and maintain those measures or capabilities. Best-in-class organizations understand their assets and installed base, monitor those assets and the personnel or machines allowed to access them, and provide ready feedback for continuous improvement. Companies with these characteristics will have better systemic resilience and overall recovery capability due to increased self-knowledge and reduced uncertainty concerning assets, threats, and weaknesses present in their systems.

A Company under assessment may have differing levels of Notation among vessels, and it may have a different level of certification granted when the Company assesses its facility or facilities. Each vessel will earn Notation on its own merits, and the Notation will reflect in the vessel's *ABS Record*. Vessels will also receive the CyberSafety Management System Certificate (CMSC) as noted previously, to show systems and cyber-enabled equipment assessed within the scope of the Notation.

The Company's Certificate of Cyber Compliance (CCC) will provide similar information as the CMSC, but for the assessed facility. If both Company and vessel(s) are assessed, vessel Notations will reflect on the highest successful Notation level achieved, as will the facility; there need not be level consistency between or among them. The vessel Notation would reflect as **CS(1/2/3)+** to denote that the Company was also assessed to the Guide specifications.

5 Specific Requirements and Capabilities for Operational Technology

A Company with mission-critical OT installed and functioning, whether aboard ship, platform or in facility, is obliged to protect the OT systems as part of their due care and due diligence associated with corporate governance, regulatory compliance, personnel safety, and asset protection needs. Because OT is frequently considered to be apart from, or separate from, information technology (IT), but often connected to IT for monitoring, remote access and control purposes, it is imperative that the process control systems, or cyber-physical systems, be protected both physically and logically.

The Company is to use appropriate regulatory and reference materials to determine their security posture. The OT specification portion of the Section 5 Capability Matrix is to address the major components of OT security and is intended to guide implementation of OT installations and operations. In developing the criteria, industry standard publications (e.g., IEC 62443, NIST Special Publication 800-82r2) are to be referenced for technical detail as required, as appropriate for the arrangement utilized. An assessment version of the OT specification, mapped to applicable industry standards (i.e., IEC 62443 and NIST Cybersecurity Framework), is to be available separately as an additional resource for OT security, to be provided as a Guidance Note for self-assessment or survey.

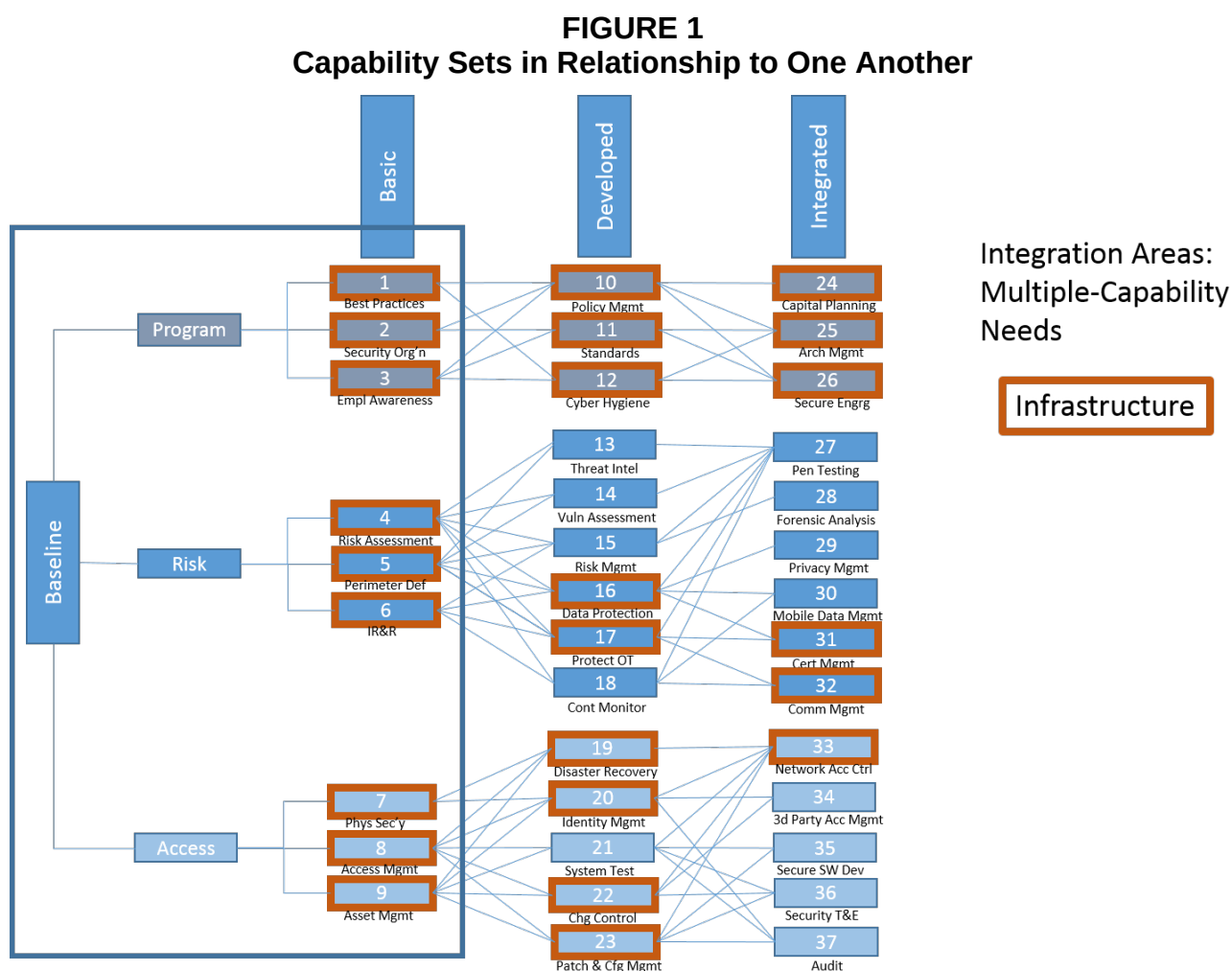
7 Use of the Capability Matrix

The Capability Matrix, in Section 5 herein, establishes marine- and offshore-specific best practices, defining and providing the organizational process specification for each capability together with the associated IT and OT specifications.

- Best practices frame the context for the individual capabilities. These notes encapsulate lessons learned and practices that are current in the capability area under examination.
- Process specifications detail how the Company may structure itself to accomplish and provide the capability in an operational setting. This specification set provides requirements for determining and shaping what the organization requires as human or system processes to implement both best practices and the technology specifications.

- The IT specification lists those requirements associated with implementation of IT within that capability. The technology specifications relate to previous capabilities, where applicable, to provide completeness through the scope from less to more complex capabilities.
- The OT specification provides those requirements associated with development, engineering and operation of OT within each capability.

To illustrate potential relationships, Section 4, Figure 1 below shows how the capability sets can connect and relate in a particular, generic implementation.



The Baseline and Basic capability sets are minimum requirements for an organization to satisfy Cybersecurity.

In this illustration, the three major subdivisions divide into the capabilities within those specific areas. The color scheme in shades of blue is meant to show commonality in each area for differentiation only.

In the Program category, for example, the Basic capability set includes Best Practices, Security Organization and Employee Awareness. These expand into the Developed level to require Policy Management, Standards, and Cyber Hygiene, then into Integrated level capabilities to include Capital Planning, Architecture Management and Security Engineering.

Each category expands from less complex capabilities into more complex capabilities, building into the Integrated set that each require inputs from several subordinate capability areas. As an example, Integrated capability 27 (Penetration Testing), when executed correctly, will derive from and integrate Perimeter Defenses (5), Threat Intelligence (13), Vulnerability Assessment (14), and System Test (21) to provide the best results. Similarly, Integrated capability 29 (Privacy Management) will combine elements of Perimeter Defenses (5), Risk Management (15), Data Protection (16) and Identity Management (20) for a complete solution.

Capabilities requirements will develop differently based on organizational needs. Some organizational development may require capabilities outside particular sets in order to address risk factors present in a specific context. In that case, the basic set of capabilities is required, along with those capabilities needed to address the risk(s) for that Company.

The Basic Capability set (including the Baseline) is the minimum requirement for a Company to satisfy Cyber due care and due diligence for the technology systems. But additional requirements may apply to an organization in its specific and unique environment. Section 4, Figure 1 above is an illustration of what capabilities may be required to satisfy security in a view toward secure infrastructure operations and management. Several Developed capabilities, and additional integrated capabilities, are shown highlighted as potential needs for the Company to operate with a degree of measurable completeness.

Specific additional “views” in a Company may require other combinations of capabilities for needs coverage. A security operations view requires additional, and different capabilities than will the secure infrastructure operations view shown.

The size of the Company, personnel complement, and numbers of fielded technology systems will drive the level of CyberSafety assessment, accomplishment and certification required to understand the Company’s security position and posture. Smaller Companies with relatively small numbers of IT and/or OT systems may be satisfied to implement and certify to the Basic level. Larger organizations with more complex systems, operations or relationships may require an implementation at the Developed level, or CS2. Large, complex Companies will probably require implementation at the Integrated level, CS3, to better accommodate their multiple needs across many subordinate organizations, units or assets.



SECTION 5 ABS CyberSafety™ Capability Matrix

1 Capability Matrix

The following tables provide the specifications necessary to satisfy Baseline, CS1/Basic, CS2/Developed and CS3/Integrated capability levels.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
Baseline Requirements			
1- Practices, Programs, and Processes			
(1) Exercise Best Practices (2) Build the Security Organization	PB2-1 The Company has personnel assigned to confirm assets and systems are received and installed in accordance with positive control and inventory or tracking procedures. PB2-2 The Company provides spaces for security personnel and operations, and security containers, safes or safe storage methods for secure storage or security data, devices or materials.	ITB2-1 Personnel are positively identified for information technology and data system duties and security, with appointment letters as required.	OTB2-1 Personnel are positively identified for operational and process control technology duties and security, with appointment letters as required.
(3) Provision for Employee Awareness and Training	PB3-1 Use broadcast emails for threat awareness and reminders of good practice. PB3-2 Employee basic training process is annual or as required, tracked and managed, and it includes - Initial (and refresher) cybersecurity training and awareness - Technology acceptable use policy, with signature - Social media training - Social engineering (Phishing, Vishing and Smishing) familiarization for threat awareness - Web use hygiene habits	ITB3-1 All users will receive standard notification banner for acceptable use and business purposes when logging into their enterprise-owned machines.	OTB3-1 All users will receive standard notification banner for acceptable use and business purposes when logging into operational, process-control systems or into interface machines that connect to operational technology systems.
2- Risk Understanding and Management			
(4) Perform Risk Assessment	PB4-1 The Company conducts periodic, or at least annual, risk assessment of current assets and risk position in their context or environment. PB4-2 The Company understands those systems, functions or data which is completely critical to safe operation of systems or assets.	ITB4-1 Perform annual (or more frequent) inventory of network-enabled and network-connected IT assets and systems.	OTB4-1 Perform annual (or more frequent) inventory of network-enabled and network-connected OT and cyber-enabled functional assets.
(5) Provide Perimeter Defense	PB5-1 Any system, workstation or device will have any inherent protective systems activated by default.	ITB5-1 Workstation or device protective systems or built-in firewalls, either hardware-based or operating system utilities, are activated by default prior to placing any system into the Company's networked environment.	OTB5-1 No system, module, component, appliance, device or application will be allowed to communicate, whether through the network or out-of-band, without explicit permission from the Company.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
	PB5-2 No system, module, component, appliance, device or application is allowed to monitor its operator, whether by camera, microphone or keyboard capture, without conscious permission of the Company or the operator. PB5-3 Every server, system, appliance, module, component, device or application will be installed with password access, and passwords shall be stored in a safeguarded location in the Company.	ITB5-2 Communication utilities in workstations or end-user systems are positively managed to confirm only authorized users control access to cameras, microphones and speakers. ITB5-3 Network infrastructure devices, especially commodity procurements, are not installed and activated in networked environments until their default protective mechanisms and methods are activated, and default accesses and passwords are changed.	OTB5-2 No operational technology or process control system is directly connected to the Internet. OTB5-3 New devices or sensors (i.e., Industrial Internet of Things (IIoT)) will be tested for performance, potential system impact and secure access methods prior to installation in operational systems.
(6) Prepare for Incident Response and Recovery	PB6-1 The Company has a process defined by which positive control of systems can be regained and personnel and asset safety maintained. PB6-2 All safety-critical systems have manual backup capabilities installed, and personnel are periodically trained in use of manual backup systems and methods.	ITB6-1 All enterprise or organizational systems have data backup and recovery capabilities installed and enabled. ITB6-2 All enterprise or organizational systems have system software master copies kept in safe storage for emergency system recovery / reload purposes.	OTB6-1 All enterprise or organizational OT and control systems have data backup and recovery capabilities installed and enabled, as appropriate. OTB6-2 All enterprise or organizational process control systems have system software master copies kept in safe storage for emergency system recovery / reload purposes.
3- Protected Resources and Accesses			
(7) Provide Physical Security	PB7-1 The enterprise physically controls all network resources within its boundaries and area of control, including portable systems or devices and network connections. PB7-2 The Company limits options for system access, device or data theft, or human information leakage by controlling visitor access in areas where unattended presence is possible, or where inadvertent eavesdropping could reveal Company operations or details. PB7-3 Video feeds from installed surveillance systems, especially Internet Protocol (IP) cameras, are not available to unauthorized or non-authenticated access. PB7-4 Manual backup methods for control of safety-critical systems are safeguarded in the same ways as are primary and automated controls in those systems. PB7-5 USB data storage or transfer devices are prohibited from physical access or use by policy, except in specified, allowed circumstances.	ITB7-1 Access control lists (ACLs) for physical possession or contact with system assets (devices, systems, workstations, servers, network connections, etc.) are established and kept up to date. ITB7-2 Physical access to spaces containing IT assets is controlled by physical barriers and devices (doors, locks) and governed in accordance with ACLs. ITB7-3 Common interface ports used for power (i.e., charging portable devices) are provided as power outlets in Company spaces in order to remove possible avenues for unauthorized or high-risk access to systems, appliances, workstations or devices. ITB7-4 Portable devices (laptops) are protected against data theft or illicit access via stolen machines by use of whole-disk encryption. ITB7-5 Infrastructure devices shall include tamper-evident seals on critical components within safety-critical or safety-relevant systems.	OTB7-1 Access control lists (ACLs) for physical contact with system assets (devices, systems, workstations, programmable logic controllers, network protocol translators, network connections, etc.) are established and kept up to date. OTB7-2 Physical access to spaces containing OT assets is controlled by physical barriers and devices (doors, locks) and governed in accordance with ACLs. OTB7-3 The Company prevents, both by policy and by physical or logical means, the ability for inappropriate and unauthorized portable device connections to OT/ICS.

Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
(8) Execute Access Management	PB8-1 New infrastructure systems shall be prepared for installation for network resource access in accordance with organizational baseline policies and procedures. PB8-2 Local (serial) connection methods are to be used, where possible, for configuration and administration tasks for infrastructure devices. PB8-3 New endpoints or user access devices shall be prepared for installation in accordance with organizational asset baseline policies and procedures. PB8-4 Personnel access to networked resources is governed by the principle of least privilege; access granted is the minimum necessary for personnel to perform their stated and defined duties.	ITB8-1 Infrastructure systems, devices, servers, applications and assets are initially configured to remove all default settings prior to installation in the networked environment, including: • Vendor default passwords are to be changed; • Administrator account passwords or access accounts are positively set upon system receipt and installation; • Administrator passwords are non-trivial and tracked by secure means in Company; • Remote access is configured only if specifically required, not be default; and • All system accesses will be tracked by logging, by unambiguous login identity or credential, to main or auxiliary repositories that contain enterprise data of consequence. ITB8-2 User endpoint systems, devices, applications and assets are initially configured to remove all default settings prior to installation in the networked environment, including: • Vendor default passwords will be changed; • Administrative privileges are not granted as to ordinary user accounts by default; • Endpoints have lateral network access or visibility only within the immediate area of their functional requirements, without default access to other systems or assets on the network; • Single sign-on (SSO) is configured for applications as required; and • Preconfigured software that uses OEM or manufacturer call-out methods will be disabled in the standard user profile to prevent unauthorized communications.	OTB8-1 All operational technology or process control system components, systems, modules, applications or appliances will have default passwords changed prior to their being activated in the Company's process control network. OTB8-2 All operational technology or process control system components, systems, modules, applications or appliances will have any remote access methods established with two-factor authentication, nontrivial passwords, and access control lists (ACLs). OTB8-3 All operational technology or process control system components, systems, modules, applications or appliances will have protocols and services (including Secure Shell (SSH)) secured against unauthorized access. OTB8-4 All operational technology or process control system components, systems, modules, applications or appliances will implement verbose logging to allow tracking of user access; resources, source IP, time/date, and files or systems accessed. OTB8-5 No operational technology or process control system components, systems, modules, applications or appliances will be configured to allow cellular data access, either one-way reporting or two-way query-response, without written permission of the asset owner. OTB8-6 No access to OT systems via USB port is allowed without prior testing of the device and/or data to be transferred by that port.