Guide for

ABS CyberSafety for Equipment Manufacturers

ABS CyberSafety® Volume 7

August 2023

GUIDE FOR

ABS CYBERSAFETY FOR EQUIPMENT MANUFACTURERS AUGUST 2023

ABS CYBERSAFETY® VOLUME 7

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

ABS Plaza
1701 City Plaza Drive
Spring, TX 77389 USA

Foreword *(1 August 2023)*

This Guide provides the requirements for equipment or computer-based systems to receive recognition for compliance as part of the ABS CyberSafety® program. The process, which requires cybersecurity vulnerabilities to be identified by the Original Equipment Manufacturer (OEM) can be applied to a digitally-enabled component or a complex system. The recognition is in the form of an ABS CyberSafety Product Design Assessment Certificate.

For new construction vessels contracted after 1 January 2024, Section 4-9-14 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)* (IACS UR E27) is to be complied with. Any additional requirements in this Guide are optional.

To receive the optional **CS-System** notation, at least one of the installed systems that provides a Primary Essential Service is to have an ABS CyberSafety PDA Certificate for a vessel or offshore unit. For further details, refer to the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Industries – ABS CyberSafety® Volume 2*.

Cyber risk can affect the supply chain at all levels. This risk can be inherited by downstream users of maritime equipment and services. While contributions to cyber risk are generally the result of non-malicious behaviors, the impacts of these risks late in the supply chain (i.e., the owner or operator) can be significant.

This Guide is primarily intended for suppliers of computer-based equipment installed in Operational Technology (OT) environments. It is secondarily intended for suppliers of computer-based equipment and associated digital infrastructure equipment supporting OT environments. The guidance herein is provided for suppliers who are committed to both (a) managing maritime cyber risk within their products; and (b) communicating potential product-related risk information to end users.

Suppliers benefit by demonstrating commitment to cybersecurity resilient computer-based systems or components. The suppliers also can offer supplier-developed or third party-tested cyber protective equipment or software which functions satisfactorily within the confines of a real-time computer-based system to mitigate cybersecurity vulnerabilities.

The owner's cyber risk analysis benefits from the disclosure of vulnerabilities, allowing the owner to select and install cybersecurity protection. To lower the owner's cybersecurity risk, the owner may install protections outside the boundary of the computer-based systems to limit or monitor data and access to the entire system. The owner may install manufacturer recommended additive cybersecurity protective equipment within the boundary of the computer-based system to limit or monitor data and access to a component or components of the computer-based system. Benefits of highly integrated cyber-enabled systems are increased safety, emerging "smart" capabilities, and crew and machinery efficiency.

The August 2023 edition of this Guide includes information on "cloud" security. OEMs may utilize cloud storage and services to collect, analyze, and present information to owners. The cloud provider, the OEMs and the customer have different security responsibilities that together can manage the entire cloud environment.

The effective date of this Guide is 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

ABS CYBERSAFETY FOR EQUIPMENT MANUFACTURERS

CONTENTS

SECTION 1
General

1 Scope *(1 August 2023)*

This Guide describes the requirements for equipment or computer-based systems to receive recognition for compliance as part of the ABS CyberSafety program. This can apply to a digitally-enabled component or a complex system. The recognition is in the form of an ABS CyberSafety Product Design Assessment Certificate.

For new construction vessels contracted after 1 January 2024, Section 4-9-14 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)* (IACS UR E27) is to be complied with. Any additional requirements in this Guide are optional.

The criteria contained in this Guide are applicable to equipment under control of a computer-based system that, in its entirety, is collectively known as a "computer-based system" or a computer-based component. Cybersecurity vulnerabilities may be introduced into computer-based systems with some digital components, network architecture, system design, and software making up the computer-based system. Cybersecurity vulnerabilities become cybersecurity risks when they are accessed by persons or computers via digital endpoints. The owner's risks from these vulnerabilities are mitigated by installing protective functions or by using hardened configurations, controlled settings, and continuously monitoring the systems. This Guide applies to systems under control by one or more computer-based system(s) such as Power Management, Dynamic Positioning, or Engine Control.

A cybersecurity vulnerability is a condition that may allow a digital device or software application to be accessed by an unauthorized digital identity or human, resulting in potential digital corruption or functional effects in the system or network. A vulnerability can exist in the equipment making up the computer-based system, third-party equipment connected to the computer-based system, and software and firmware executing on the components. These vulnerabilities can be eliminated with firmware or software updates, configuration changes, privilege changes, or architectural modifications. When found early in asset construction and system installation, integrators, shipyards, and owner/operators can manage related risks and/or embedded risk management solutions more efficiently and economically.

An ABS CyberSafety Product Design Assessment for a digitally-enabled component or complex system documents known cybersecurity vulnerabilities to facilitate an asset owner's cybersecurity risk analysis and remediation. The Original Equipment Manufacturer's (OEM) product receives an ABS CyberSafety Product Design Assessment Certificate when it meets the requirements set forth in this publication.

The equipment may have cybersecurity vulnerabilities that may be mitigated by installing tested architecture equipment (including but not limited to routers and data diodes) or software (firewalls). Vulnerabilities also can be eliminated with software patches or updates. By understanding the unresolved vulnerabilities, the owner can choose to install hardware or other protective functions, modify architectures, or change processes to decrease the known vulnerability, and thus mitigate the owner's associated cybersecurity risk.

Operational Technology, or "OT" systems, are computer-based systems that control production or operational systems. These cyber-physical systems control processes and systems and impact safety in their environments as they control the physical behaviors of connected equipment. They generally communicate with Information Technology (IT) general-purpose networks to provide sensed operational data to management personnel. Computer-based systems extend to the connected network and the components, as well as any IT equipment used to display data and for operator control.

Computer-based systems may be composed of the OEM's and sub-supplier's computer-based systems, computers, servers, or cyber-enabled and networking infrastructure components. Digitally-enabled Commercial-Off-The-Shelf (COTS) components may be installed in the computer-based system as well.

2 OEM Company Level Requirements *(1 August 2023)*

The development environment influences component selection and programming. The environment is controlled by the OEM's policies and procedures, product change management, cybersecurity training, risk management, and other management processes to govern product development and evolution. Because of the impact these documented processes have upon product development and evolution, ABS is to review these processes (See Section 1, Table 1).

The OEM has the greatest insight into their product as they can monitor their supply chain, select components, document cybersecurity vulnerabilities, and install or recommend cybersecurity protections.

The OEM can verify if a component is listed in the NIST National Vulnerability Database or the OEM can purchase components that are cybersecurity certified with all other considerations being met. The OEM is to declare any known cybersecurity vulnerabilities to downstream users. The integrator, shipyard and owner may then review the declared vulnerabilities of the computer-based system and determine cybersecurity protective equipment to install at the boundary of the computer-based system to mitigate the risk. It is recommended to involve the OEM when installing cybersecurity protective equipment within the boundary of the real-time computer-based system, because potential data and command latency caused by cybersecurity protective equipment may affect system safety and performance.

Computer-based systems are relevant to safety in their environments since the equipment operates in real-time, and thus time delays in commands and data potentially caused by cybersecurity protective equipment are a concern. It is recommended that the OEM test cybersecurity protective equipment that functions within acceptable parameters for downstream integrators, shipyards and owners to install within the boundary of the computer-based system to mitigate any declared vulnerabilities.

The functional description, equipment list, topology drawing, and accessible connections of the computer-based system are addressed in this Guide, to address vulnerabilities introduced by digital device connections and human interface access. The remote connections and wireless networks are addressed with potential vulnerabilities (rogue wireless connections and Internet attacks on remote connections) and controls the OEM puts in place to mitigate access to wireless devices and access points and remote connections.

The component or computer-based system is to be programmed, developed, tested, and maintained in a cybersecure-controlled environment to minimize the introduction of cybersecurity vulnerabilities during these activities. The OEM is to be a certified ABS CyberSafety Service Supplier, in which case ABS will review documents for compliance as listed in Section 1, Table 1.

TABLE 1
OEM Company Level Requirements *(1 August 2023)*

	Recognized ABS CyberSafety Service Supplier
Requirements:	• Location Software is Developed (2/2.1) • Cybersecurity Standard (2/2.2.1) • Cyber Security Office (2/2.2.2) • Incident Response Team (2/2.2.3) • Cybersecurity Policies and Procedures (2/2.2.4) • Internal Risk Management (2/2.2.5) • Cybersecurity Training (2/2.2.6) • Product Change Management (2/2.2.7) • Third Party Involvement in Programming (2/2.2.8) • Copies of Certificates (2/2.3) • ABS Audit (2/2.4 and 4/3) • Annual Reports (4/4)
Required for:	1) Computer-based system components requesting PDA and installed in: • Essential Services or Safety Systems • Category II or III Systems (see 2/1.1) 2) Cloud Security
Suitable for:	• Complex functionality (as defined by OEM) • Frequent updates (OEM request a PDA revision for updates to the associated equipment PDAs) • Frequent customization • Large number of components requiring ABS approval • Cloud Security
Eligible for:	• ABS CyberSafety Product Design Assessment • ABS CyberSafety Product Design Assessment with Cloud Security Endorsement

3 Equipment Level Requirements *(1 August 2023)*

The OEM may request an ABS CyberSafety Product Design Assessment (PDA). In addition, if the OEM uses the services of a cloud provider, the OEM may request ABS to review the applicable requirements of Cloud Security in Section 5. In this case, upon approval, the ABS CyberSafety PDA certificate will have an endorsement for compliance with the ABS Cloud Security requirements.

The required documentation for computer-based systems and components applicable to the ABS CyberSafety PDA and Cloud Security are summarized in Section 1, Table 2.

TABLE 2
Equipment Level Requirements *(1 August 2023)*

	ABS CyberSafety PDA	*Additions for Cloud Security*
Applicability and Limitations:	Applicable to many applications with Service Restrictions listed on ABS CyberSafety PDA Certificate.	
Requirements: ***Note:*** Primary and Secondary Essential Systems and Category II and III hardware that executes the OEM's ABS CyberSafety PDA program is to be ABS approved. The hardware approval is subject to Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* for the equipment PDA and the applicable Rules.	Vulnerability Report (3/2.1) consisting of: • Cybersecurity Vulnerability Analysis (3/2.2) • Description of known OEM cybersecurity vulnerabilities not mitigated by the OEM cybersecurity functions • OEM installed cybersecurity functions (hardware and software) • OEM login requirements to OEM equipment and cybersecurity functions • Computer-based system or component description documents (3/2.3) • Sub-supplier functionality descriptions, vulnerabilities descriptions, and topology drawing, as reported by sub-supplier, if any. • Sub-supplier's remote connection vulnerabilities, as reported by sub-supplier, if any. • OEM's topology drawing (3/2.4) • Anti-malware Scans and Software Backups (3/2.5)	Information to be provided by OEM: • Cloud provider's audit report and certificates (5/2.1) • Cloud data security (5/2.2) • Cloud provider's and OEM information (5/4.1.1) • Access requirements (5/4.1.2) • Server and runtime logs (5/4.1.3) • Client access software (5/4.2) • Software updates (5/4.3) • Encryption key management (5/5)
Type Test:	See Subsection 4/1 for the CyberSafety PDA Type Test ***Note:*** There may also be equipment hardware Type Testing required per Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* for the hardware PDA.	No additional Type Tests for Cloud Security

4 Limitations *(1 August 2023)*

i) ABS CyberSafety for Equipment Manufacturers is applicable to computer-based equipment, local and remote Human Machine Interfaces (HMI), and supporting IT systems connected to the computer-based equipment system(s) or network(s) in functional supporting roles. This includes the operating system, control system(s), and computers residing on the computer-based equipment network(s) and special-function IT systems that may affect performance of the computer-based system being approved. The programmed functionality of the system is not included in this Guide. Therefore, the programmed actions or purpose of the computer-based system is not reviewed or included as part of the ABS CyberSafety PDA.

ii) Modifications and actions by others affecting the computer-based system or its cybersecurity functions applicable to the as-described and assessed computer-based system or component, when applied by any party other than the OEM or submitter, including the owner, are not covered by the ABS CyberSafety PDA. Only the as-delivered computer-based system and the as-described components and cybersecurity performance to either the integrator, shipyard, or owner is covered by the ABS CyberSafety PDA. Additions to or modifications of the computer-based system and/or its associated network(s) by any other party to the computer-based system, OT or IT networks are not covered.

iii) The ABS CyberSafety PDA is based upon the OEM's documentation listing disclosed vulnerabilities and OEM cybersecurity described performance at the time of application.

5 Definitions, Abbreviations, and References *(1 August 2023)*

5.1 Definitions *(1 August 2023)*

Accessible Physical Ports. Ports (such as RJ45 and USB) that are not physically protected by cabinets (lockable or not) or disabled, located in controlled spaces, or normally monitored or locked rooms.

Application Program Interface (API). An application that enables programs to interface (exchange data and commands) with another computer-based system.

Bastion Host. A computer with limited programs and applications used exclusively for administrative purposes of the cloud.

Category II and III Systems. Defined in Section 4-9-3 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)*. These correspond to IL2 and IL3 systems, as defined in 3/5.3 of the ABS Guide for Software Quality Management (SQM). Category II is defined as "eventually lead to dangerous situation" while Category III is defined as "immediately lead to dangerous situation".

Cloud Provider. The company with hardware and software infrastructure offering cloud services to the public with access via the Internet.

Commercial-Off-The-Shelf (COTS). Denotes a component provided by a commercial supplier that is used as is, adapted, or configured for use, but not programmed specifically for the OEM's project.

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

Computer-based System. The equipment or system subject to the ABS CyberSafety PDA. A computer-based system performs a specified function, is commonly composed of electromechanical equipment connected to a single computer-based system or multiple computer-based systems, is a subset of Operational Technology (OT), and is usually a cyber-physical system controlling physical equipment in real time processing. The computer-based system's functionality is programmed for various conditions and the functionality is called OT Functionality.

Current Equipment Manufacturer. The current programmer of a computer-based system that may or may not be produced by the OEM.

Cybersecurity Function. Functions or controls that provide either physical (routers, programmed switches) or logical (software, i.e., firewalls) cybersecurity protection to mitigate vulnerabilities.

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

Essential Services (Primary and Secondary). Services considered necessary for continuous operation to maintain propulsion and steering (primary essential services), non-continuous operation to maintain

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

Factory Acceptance Test (FAT). Testing of the computer-based system generally focused on testing the OT functionality, usually at the manufacturer's facilities.

Hypervisor. A type of computer software, firmware, or hardware that creates and runs virtual machines.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Integrity Level. An OEM-assigned value from 0 to 3 denoting the severity of computer-based system failure as defined in the ABS *Guide for Integrated System Quality Management (ISQM Guide)* based upon safety, environment, and asset's mission considerations. See Section 3, Table 1 of the *ISQM Guide*.

Media Access Control (MAC). Address for Ethernet hardware address assigned by the manufacturer of network cards and other layer 2 devices (such as switches) of the OSI model.

Node. A digital communications connection point capable of transmitting, receiving, or creating information over a communication channel. The node can use serial, network, and various protocols for passing digital information.

Original Equipment Manufacturer (OEM). A supplier that is the primary provider of a computer-based system and programmer of the system or component.

Operational Technology (OT). Automated systems (cyber-physical), including hardware and software, that perform direct monitoring and/or control of physical devices, processes, or events. It is a superset of computer-based industrial control systems that includes monitoring, sensing, and human interface devices, as applicable to an installation.

OT Functionality. The programmed actions and purpose of the computer-based system and how the collective system is programmed during normal, degraded, and failed states or conditions.

Platform as a Service (PaaS). The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

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) (see the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety® Volume 2)*.

Service Level Agreement. The agreement between the cloud provider and the OEM details the cloud infrastructure and services and what is to be managed and provided by the OEM. This agreement contains security and performance compliance for the cloud provider.

Service Category. General type of cloud services offered by cloud providers span from a full functioning server to just server hardware and basic software connections.

Service Supplier. Voluntary recognition for qualified service suppliers who offer specialized services and enhance existing marine and offshore safety practices offered by ABS.

Simple Connection. A direct digital communications path between one piece of equipment and one or more other pieces of equipment (not networked), but not to the Internet.

SOC 1 Report. A Service Organization Controls (SOC) audit report from the American Institute of Certified Public Accountants, the SOC 1 report is focused on financial transaction security and SOC 2 Report IT security. The entirety of the SOC 1 report is restricted, with ABS seeking indication of compliance and not the report itself.

SOC 2 Report. A Service Organization Controls (SOC) audit report from the American Institute of Certified Public Accountants, the SOC 2 report is focused on IT security (security, availability, process integrity, confidentiality, and privacy of data processed by the cloud provider). The entirety of the SOC 2 report is restricted, with ABS seeking indication of compliance and not the report itself.

SOC 3 Report. A Service Organization Controls (SOC) audit report from the American Institute of Certified Public Accountants, the SOC 3 report is a public facing SOC 2 report.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software Quality Management (SQM). The requirements for notation(s) according to the ABS *Guide for System Quality Management (SQM Guide)*.

Sub-supplier. A company providing digitally-enabled hardware that is programmed to meet the OEM's requirement(s) with a sub-system or programmed component. Excludes COTS and sub-suppliers who provide services or training on behalf of the OEM.

Sub-system. A programmed digitally-enabled set of components supplied to an OEM as a sub-component of the OEM's computer-based system as a custom-made solution. It excludes instrumentation, electrical breakers, Commercial-Off-The-Shelf (COTS) components connected to a wireless or wired network, and mechanical equipment (including but not limited to steel, bolts, and concrete).

Thin Client. A computer that runs from resources stored on a central server instead of a localized hard drive.

Thin Client Software. Software that uses the resources of the connected server rather than local resources.

Very Large Network. A direct digital communication path between cyber-enabled equipment or network(s) to a node or endpoint accessible to a very large number of digital identities, such as the Internet.

Vulnerability. A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-53. It is a weakness that allows a digital device, endpoint, or software application to be accessed by an unauthorized digital or human identity and digitally corrupts or affects the functionality of the system or network.

5.2 Abbreviations *(1 August 2023)*

API : Application Program Interface program

Apps : Application programs

CEM : Current Equipment Manufacturer

COTS : Commercial-Off-The-Shelf products

CSO : Cyber Security Office

CVSS : NIST NVD Common Vulnerability Scoring System (CVSS)

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name Server

FAT : Factory Acceptance Test

HMI : Human Machine Interface

IaaS : "Infrastructure as a Service" Service Category

IIOT : Industrial Internet Of Things

IL : Integrity Level from Section 3, Table 1 of the ISQM Guide

IOT : Internet Of Things

IRT : Incident Response Team

IT : Information Technology

MAC : Media Access Control

MAoC : Manufacturers Affidavit of Compliance (MAoC)

NIST : National Institute of Standards and Technology

NIST NVD : National Institute of Standards and Technology, National Vulnerabilities Database (https://nvd.nist.gov/)

OAuth 2.0 : The industry-standard protocol for authorization. This specification and its extensions are being developed within the Internet Engineering Task Force OAuth Working Group. See www.oauth.net.

OEM : Original Equipment Manufacturer

OSI : Open Systems Interconnection

OT : Operational Technology

PaaS : "Platform as a Service" Service Category

PDA : ABS Product Design Assessment Certificate as defined in the ABS *Rules for Conditions of Classification (Part 1)*

PPS : Ports Protocols and Services

SaaS : "Software as a Service" Service Category

SOC 1 : Service Organization Controls report 1

SOC 2 : Service Organization Controls report 2

SOC 3 : Service Organization Controls report 3

SQM : Software Quality Management

5.3 Recognized Industry Standards *(1 August 2023)*

ISA/IEC 62443-1 through 4 *Industrial Network and System Security*

ISO 27001 Security techniques – *Information security management systems – Requirements*

ISO 27002 Security techniques – *Code of practice for information security controls*

MIL-DTL-32613(SH) *Detail Specification, Controller, Auxiliary-System, Naval Shipboard Use*

NIST CSF *Framework for Improving Critical Infrastructure Cybersecurity*

NIST SP 800-82 *Special Publication – Guide to Industrial Control Systems (ICS) Security, Revision 2*

NIST SP 800-53 *Special Publication – Recommended Security Controls for Federal Information Systems and Organizations*

5.4 References *(1 August 2023)*

ABS *Rules for Conditions of Classification (Part 1)*

ABS *Rules for Building and Classing Marine Vessels*

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

ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Industries – ABS CyberSafety® Volume 2*

ABS *Guide for Software Quality Management*

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

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

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

Cybersecurity Capability Maturity Model (C2M2), Office of Cybersecurity, Energy Security, and Emergency Response, US Department of Energy

International Association of Classification Societies, Rec 166, *Recommendations on Cyber Resilience, July 2020*

International Association of Classification Societies, UR E26, *Cyber Resilience of Ships, April 2022*

International Association of Classification Societies, UR E27, *Cyber Resilience for On-board Systems and Equipment, April 2022*

SECTION 2

OEM Company Level Requirements

1 General *(1 August 2023)*

Products, components, and computer-based systems are to be developed in a cybersecure environment. ABS is to review the OEM's internal policies, procedures and cybersecurity processes, risk management and change management compared to the OEM's declared foundational standard.

If owners are currently using firms who are not ABS Recognized Service Suppliers, these firms may be qualified as ABS Recognized Service Suppliers by submitting an application through the nearest ABS Survey Office. See "Service Suppliers" on the ABS website www.eagle.org for additional information, the process for applying to be a recognized Service Supplier, and the database of approved suppliers.

The ABS CyberSafety PDA is provided based on a review of OEM documentation for compliance with pertinent Rules or Guides and this Guide.

1.1 OEMs Who Desire to Become a Recognized Service Supplier for ABS CyberSafety *(1 August 2023)*

The OEM submits a Service Supplier application noting "ABS CyberSafety" on the application. The OEM is to submit documents listed in Subsection 2/2. Upon meeting the requirements and passing the audit, ABS will issue the ABS CyberSafety Service Supplier Recognition to the OEM. Section 2, Figure 1 shows the process to receive the ABS CyberSafety Service Supplier Recognition.

The Service Supplier Recognition is specific to one OEM location.

Recognition as a Service Supplier is required for:

i) Computer-based system components installed in primary and secondary essential services (1/5.1) or safety systems delivered with an ABS CyberSafety PDA.

ii) Cloud Security. Cloud Security is sought for cloud-based data storage, processing, or services the OEM is offering to their clients for marine and offshore data.

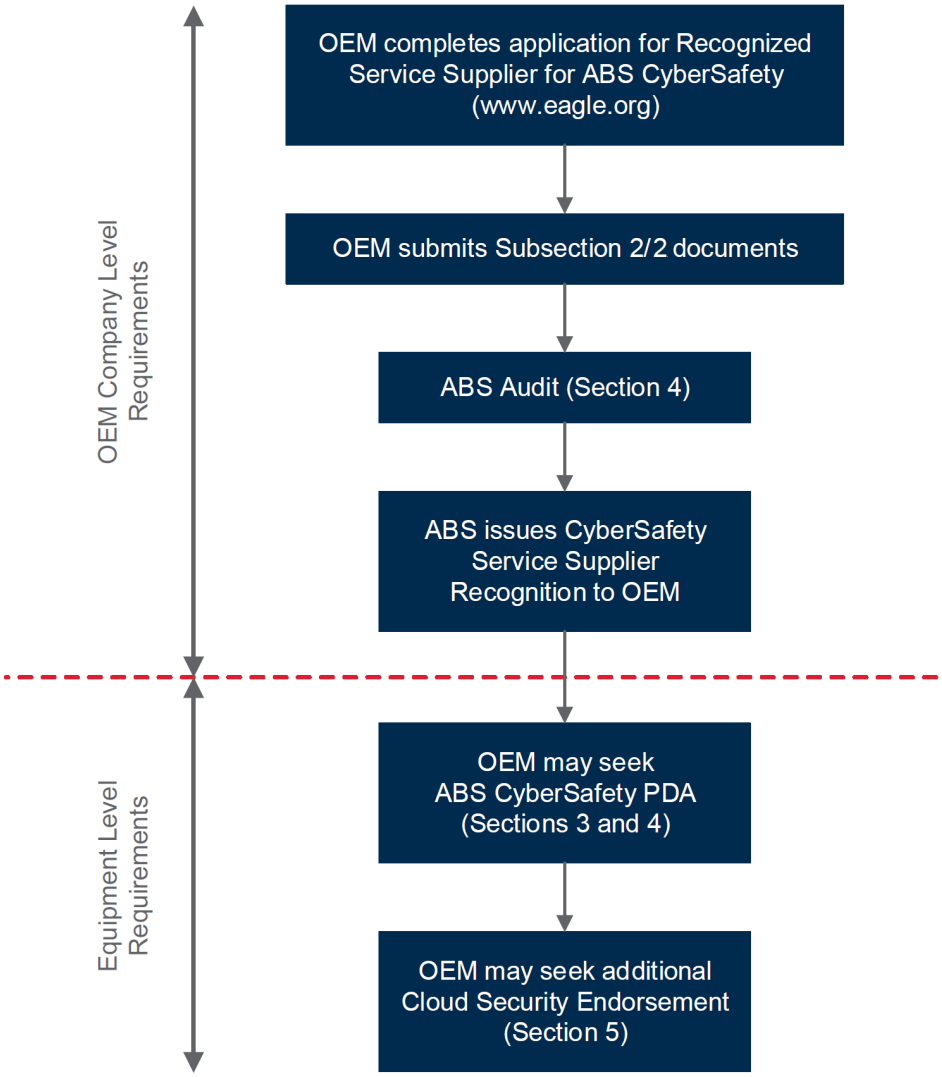
iii) Computer-based system components installed within systems listed in System Categories II and III as defined in Section 4-9-3 of the *Marine Vessel Rules* delivered with an ABS CyberSafety PDA.

If the OEM's Service Supplier Recognition is invalidated, for any reason, the ABS CyberSafety PDAs associated with systems listed in 2/1.1i) through iii) will be suspended until the Service Supplier Recognition is revalidated.

Only recognized ABS CyberSafety Service Suppliers shall update CyberSafety PDA for major updates or changes to software or hardware.

The ABS CyberSafety Service Supplier recognition is subject to annual audits, and the OEM is to submit an annual report.

FIGURE 1
ABS Recognized Service Supplier Process *(1 August 2023)*



2 OEM Recognized Service Supplier *(1 August 2023)*

2.1 Locations where OEM Software is Developed *(1 August 2023)*

The OEM is to submit documents for all locations where control system software is developed, tested, and maintained for the computer-based system(s) or components under consideration for an ABS CyberSafety PDAs.

2.2 OEM Cybersecurity Documents to be Submitted for Review

OEM's revision-controlled documents which address the following are to be submitted:

2.2.1 OEM's Preferred Cybersecurity Standard

The OEM is to state the foundational standard or combination of standards used in development of their cybersecurity methodology. See 1/5.3.

2.2.2 OEM's Internal Cyber Security Office (CSO)

The OEM is to identify a person, organization, or office responsible for the internal IT and OT cybersecurity of the OEM's facilities in which product development is performed, as well as denote cybersecurity protections embedded in the product, as applicable. The OEM is to submit the CSO documentation listed below:

i) Mission statement of the CSO with defined cybersecurity goals for computer-based systems

ii) Names or titles of the CSO members

iii) Roles and responsibilities of CSO members, including approvals and authorities

iv) OEM's organizational chart showing the CSO

The following are to be available to ABS upon request:

v) CSO audits or reviews

vi) Corporate technical risk tolerance and technical risk evaluation documentation

2.2.3 OEM's Incident Response Team Organization (IRT) *(1 August 2023)*

For the computer-based system under consideration for the ABS CyberSafety PDA:

i) The OEM is to have an organization, office or person(s) who are responsible for providing support to clients who require assistance recovering from a cyber-related software failure.

ii) The OEM is to develop an Incident Response Plan with a recovery procedure

Note: The OEM is required to notify ABS per the agreed Terms and Conditions of the issued PDA.

iii) The OEM is to submit:

- ***a)*** Incident Response Policy and Procedure
- ***b)*** Mission statement of the IRT
- ***c)*** Roles and responsibilities of team members, including approvals and authority

iv) The following are to be available to ABS upon request:

- ***a)*** Incident Response Plan including the recovery procedure for the computer-based system [2/2.2.3ii)].
- ***b)*** Indications of periodic performance of tabletop exercises focused on client recovery from a cyber incident.
- ***c)*** Findings of any incident response investigation of a reported computer-based system failure, with approved remedies and implementation timeline, or the procedure for such investigation.

2.2.4 OEM's Cybersecurity Policies and Procedures

The OEM is to submit:

i) General Cybersecurity Policies and Procedures addressing:

- ***a)*** Physical and access security
- ***b)*** Acceptable use of OEM's digital devices including portable devices

c) Digital access, registration, and de-registration of OEM's personnel and contractors

1) Role-based least functionality assigned and limitation

2) Account management

3) Access control to OEM's IT and OT resources

4) Login identification and authentication

d) Protection of information (during processing, storage, and data breach response)

ii) Network Security Policies and Procedures

a) Remote access (into OEM's network)

b) Use of wireless and mobile devices at the client's site

2.2.5 OEM's Internal Risk Management

The OEM is to make available to ABS, upon request:

i) Enterprise and product cyber risk assessment policies and procedures.

ii) Documents describing periodic cyber risk assessment of enterprise business systems with consideration of controls in place to manage identified risks.

iii) Documents describing periodic technical cyber risk assessments of products, including risks identified, risks tolerated or accepted, controls embedded in products to manage identified risks, and controls recommended for managing risks after product implementation.

If the OEM has a current ISO 27001 Certificate, items 2/2.2.5i) and 2/2.2.5ii) are not required.

2.2.6 Cybersecurity Training *(1 August 2023)*

The OEM is to conduct periodic cybersecurity training of office and field personnel.

i) The OEM is to submit:

a) Cybersecurity awareness and training policy

b) The titles of provided training topics and titles of personnel who periodically receive the training. The training is to address:

1) Cyber hygiene (employees and contractors)

2) Use of portable digital devices (e.g., phone, memory devices, portable hard drives)

3) Security of company and client data

c) Records or logs of completion of training by personnel and contractors

d) On-boarding cybersecurity training topics for new personnel (if different from above)

e) Schedules of periodic refresher cybersecurity and change management policies and procedures training

2.2.7 OEM Change Management and Configuration Control

The OEM documents and implements change control procedures for internal enterprise business systems, product hardware, embedded software and embedded cybersecurity controls, as well as production, testing, installation, and maintenance processes. The procedures are to define major and minor revisions, as well as extensive updates or significant modifications. The OEM is to denote:

i) Change management policy and/or procedure for hardware and software of computer-based systems

ii) Documentation indicating tracking of change management from request through implementation, upon request by ABS. The documentation is to detail:

a) Approval flow

b) Change document tracking

c) Internal testing

d) Implementation on client's platforms

iii) Description of software change management program or practices to manage inherent evolutionary conditions, denoting:

a) Changes to fielded control system requirements

b) Revisions to and updates in fielded control system applications

c) Fielded software incompatible with recommended or critical security updates

d) Low-impact replacement of fielded but unsupported control system software version(s)

2.2.8 Third Party Involvement in Programming of the OEM's Software

If a third party is involved from a remote location in the programming or software maintenance for the computer-based system being considered for an ABS CyberSafety PDA, then that company or companies are to be involved and provide the required documents listed in 2/2.2.1 through 2/2.2.7.

i) If the third party uses the same policy and procedures as the OEM, the third party is to state that they use the same policies and procedures as the OEM.

ii) If the third party uses different policy and procedures, the OEM is to submit documents listed (2/2.2.1 through 2/2.2.7) for the third party.

iii) The OEM is to provide a document detailing how the OEM receives, verifies, and tests software obtained from third parties.

2.3 Copies of Certificates

If the OEM holds any of the following certificates, copies are to be submitted.

i) ISO 9001 or equivalent

ii) ISO/IEC 27001

iii) ISA/IEC 62443

iv) ISASecure® Certificates (IEC 62443 conformance certificate)

In addition, any other cybersecurity certificates are to be noted and submitted.

2.4 ABS Recognized Service Supplier Initial Audit *(1 August 2023)*

After the OEM has closed all technical comments from the ABS engineering review, the OEM is to contact the local ABS Survey office for the audit. The initial audit requirements are listed in Subsection 4/3.

2.5 ABS Recognized Service Supplier *(1 August 2023)*

Upon the OEM meeting the requirements of 2/2.2 and the audit specified in 2/2.4 above, the OEM is to receive the ABS CyberSafety Service Supplier recognition and may proceed with the equipment document review (Section 3). The OEM is to complete a "Request for Certification – ABS Type Approval Product Design Assessment (PDA)" application (www.eagle.org) for the computer-based system or component to be design assessed.

SECTION 3

Equipment Level Requirements

1 General *(1 August 2023)*

Component selection, overall system design, architecture, and software may inadvertently introduce cybersecurity vulnerabilities that can be mitigated by appropriate cybersecurity controls. Equipment is reviewed for Product Design Assessment.

For additional Cloud Security see requirements in Section 5.

1.1 ABS CyberSafety PDA

The OEM is to submit a "Request for Certification – ABS Type Approval Product Design Assessment (PDA)" application (www.eagle.org) for the computer-based system or component to be design assessed.

1.2 New or Updated Product Design Assessment (PDA) *(1 August 2023)*

i) If the hardware equipment, which includes the computer-based system, has a valid ABS PDA or Type Approval Certificate, then see 3/1.2iii)b).

- ***a)*** The ABS CyberSafety application is to list the associated equipment PDAs or Type Approval number(s) and system identifier(s) to which the OEM is applying this ABS CyberSafety PDA Certificate.

ii) If the equipment, which includes the computer-based system is installed in Primary or Secondary Essential Systems or Category II or Category III systems.

- ***a)*** The CyberSafety PDA system does have a cascading effect upon a Primary or Secondary Essential System or Category II or Category III systems.

iii) If the computer-based controller hardware does not have the ABS approval, two application forms to request PDA are to be submitted:

- ***a)*** The first application is to request an equipment (hardware) PDA for the system, CPU, or controller component following Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)*, and is applicable to:
  - ***1)*** Hardware installed in Primary or Secondary Essential Services system, Category II or Category III systems.
  - ***2)*** CyberSafety PDA systems connected to Primary or Secondary Essential System, Category II or Category III systems. The OEM is to provide a clear statement that upon failure the CyberSafety PDA system will have no cascading effect upon those systems.
- ***b)*** The second application is to request an ABS CyberSafety PDA for the computer-based system or component following this Guide.

iv) If endorsement for Cloud Security is desired, the OEM is to indicate the same in the application for the ABS CyberSafety PDA. In this case, the additional requirements in Section 5 are applicable.

2 Vulnerability Report *(1 August 2023)*

The Vulnerability Report is a revision-controlled document that is listed on the ABS CyberSafety PDA. It is to be made available to the integrator, shipyard, or owner upon request from the OEM. The Vulnerability Report consists of functionality description, Controlled Equipment and Software Registry, Vulnerability Assessment, installed and/or recommended cybersecurity protective functions (hardware or software), topology drawing of OEM connected components network, potential vulnerabilities associated with any wireless networks and remote connections, and controls associated with wireless networks and remote connections. The Vulnerability Report serves downstream users by providing cybersecurity risk analysis and cybersecurity risk profiling to determine if and where to install cybersecurity protective functions to mitigate the cybersecurity risk.

2.1 Vulnerability Report *(1 August 2023)*

The OEM is to report cybersecurity vulnerabilities as reported by sub-suppliers concerning their sub-systems and sub-components provided to the OEM for installation in the computer-based system.

A Vulnerability Report is to be listed for each computer-based system listed on the ABS CyberSafety PDA.

i) The OEM is to submit a Cybersecurity Vulnerabilities Report of the OEM's computer-based system addressing:

a) Cybersecurity Vulnerability Analysis (3/2.2)

b) Description of known OEM cybersecurity vulnerabilities that are not mitigated by the OEM cybersecurity functions. If the OEM is planning to introduce mitigating controls, expected implementation description and timeline are to be included

c) OEM installed cybersecurity functions (hardware and software)

d) OEM login requirements to OEM equipment and cybersecurity functions:

1) OEM and user passwords requirements:

- Minimum length and complexity (required special characters for OEM's and owner's personnel) and reuse of passwords
- Password lifetime restrictions or time till expiration
- Number of login attempts till disabled or delay time to retry

e) Computer-based system or component description documents (3/2.3).

f) Sub-supplier functionality descriptions, vulnerabilities descriptions, and topology drawing, as reported by sub-supplier, if any.

g) Sub-supplier's remote connection vulnerabilities, as reported by sub-supplier, if any.

h) OEM's topology drawing (3/2.4).

2.2 Vulnerability Analysis

2.2.1 Items to be Submitted *(1 August 2023)*

The OEM is to perform a Cybersecurity Vulnerability Analysis where the OEM reviews each OEM-installed accessible digital endpoint and connected equipment for:

i) Vulnerability Analysis (3/2.2.2), listing cybersecurity functions or protections

ii) Controls applied to potential vulnerabilities from access by a digital device or human to each digital endpoint.

iii) Controls applied to potential vulnerability from each digitally-enabled connected component.

iv) Controls applied to potential vulnerability from safety or mission-completion consequence of unauthorized access.

v) Physical or logical protection or monitoring provided or recommended for endpoints.

vi) Controls applied to potential connection to or access by an unidentified or unauthorized digital device (wireless, Internet, via local ports).

vii) Security implemented by OEM for OEM's personnel and digital devices for local and remote access (passwords, two-factor authentication, etc.), both prior to delivery and during field maintenance activities.

viii) Security implemented by OEM for access by end user's personnel and digital devices (limited access privileges, passwords, two-factor authentication, etc.).

ix) Known vulnerabilities of hardware, embedded firmware, software, and APIs.

x) Tested and OEM approved cybersecurity functions installed to mitigate known vulnerabilities:

a) It is recommended that the OEM list of tested and OEM recommended or advised third-party cybersecurity functions that is not installed on the equipment or system is included.

b) It is recommended that the OEM list of untested, but OEM-recommended cybersecurity functions, if any, which may mitigate known vulnerabilities for post-installation applications.

2.2.2 Analysis Process

It is recommended that the OEM follow the Failure Mode and Effects Analysis (FMEA) process to analyze nodes for vulnerabilities listed in Section 3, Table 1 for the computer-based system. Section 3, Table 1 was extracted, in part, from NIST SP 800-82.

Section 3, Table 1 is to be used for the vulnerability analysis of the nodes and connections for the computer-based system or component connections. The OEM may add additional *Risk Contribution Class* items.

TABLE 1
OEM's Vulnerabilities Table *(1 August 2023)*

Taxonomy Class ID	*Risk Contribution Class*	*Notes*
F1	List known vulnerabilities in embedded software and firmware and the component each vulnerability is found in. List if found in NIST NVD and the CVSS score. List any cybersecurity functions installed by the OEM to mitigate the vulnerability. List any recommended but not installed cybersecurity functions. (See Note)	The NIST NVD CVSS assists with protection and criticality determination.
F2	Provide the certificate of any components within the computer-based system that are cybersecurity certified by UL, CSA, or other organization and delivered with an ABS CyberSafety PDA scope of supply.	

Taxonomy Class ID	*Risk Contribution Class*	*Notes*
F3	OEM to review the number of critical and non-critical connections to components or other computer-based systems for cascading events and document results of review and remedies to reduce potential of cascading events. If the OEM system is part of a Primary or Secondary Essential Services system or Category II or III systems, the hardware is to be approved by ABS. See 3/1.2.	Probability of critical systems being affected by cascading events increases with the number of critical and non-critical computer-based systems that share common dependency. OEM is to state if safety analysis indicates impact on Primary or Secondary Essential Services or Category II or III systems or not. If impact is suspected, the OEM is to be a CyberSafety Service Supplier and hardware is to be ABS approved. If not, the OEM is to state no effect on above systems.
F4	OEM to review vulnerabilities that may increase with connection path complexity and any remedies or cybersecurity controls installed.	Proliferation of endpoints or nodes related to connection complexity (discrete, simple, complex, or Very Large Network (VLN))
F5	OEM to review the potential vulnerabilities introduced with remote OEM connection(s) and any OEM installed controls to mitigate the vulnerabilities.	Supplier remote access maintained by wireless communications (Internet, proprietary satellite)
F6	OEM to review the potential vulnerabilities introduced with local OEM local access and the controls to mitigate the vulnerabilities.	Supplier onboard access to maintain the computer-based system using PCs, portable devices, communications and manual means
F7	OEM to review potential vulnerabilities associated with insecure or unprotected wireless networks and access, including Wi-Fi, Bluetooth, mobile phone, etc.	Mutual authentication between clients and computer-based system's access points so that wireless clients do not connect to rogue access points and rogue clients do not connect to computer-based system's wireless access point(s).
F8	OEM to review wireless data encryption requirements, as required.	
C1	OEM to review unprotected accessible physical endpoints.	RJ45 and USB ports not protected by access controls or located in locked or restricted access rooms.
C2	OEM to review unprotected endpoints by cabinet enclosures.	Endpoints that are not protected by access controls, restricted cabinet enclosure, or controlled access room.
C3	OEM to review unprotected endpoints by in situ device, alarm or construct.	Device disconnection from a port alerts the operator of the disconnection.
C4	OEM to review unprotected endpoints not protected by login and password.	Accessible physical port(s) for OEM and/or crew access.
C5	OEM to review for unprotected endpoints not protected by digital device (ID dongle key) carried by personnel to provide identification, two-factor identification (employee number, organizational role), or other methods to prevent humans or digital identities from gaining access to the system.	

Taxonomy Class ID	*Risk Contribution Class*	*Notes*
ID1	OEM to review for logically unprotected endpoints without some sort of identity challenge: *i)* Identity confirmed by biometric *ii)* Identity confirmed by digital device, ID, key or token *iii)* Identity confirmed by username, password, entry code *iv)* Identity confirmed by documented organizational role *v)* Identity confirmed by monitored communications characteristics, black/white lists, expert system rejection, multifactor	
ID2	OEM to review for digital device accessing endpoint (consider OEM's and owner's personnel): *i)* Access by a digital device not configured for use in accordance with OEM's policy or best practices *ii)* Access by an unscanned digital device for use in accordance with OEM's policy and/or best practices	
O1	OEM to review computer-based system vulnerabilities if the computer-based system is dependent upon the IT system for any service.	
O2	OEM to review computer-based system boundary defined as clearly as possible within limitations of scope of delivery.	Does not apply to components.
O3	OEM to review the vulnerabilities associated with unutilized or unused network Ports, Protocols and Services (PPS) within the computer-based system. The OEM is to declare if PPS are restricted or not.	It is recommended that unused PPS be disabled or per owner's requirements.
O4	OEM to review for configuration of network switches which may allow for switching loop interfaces storm vulnerability.	i.e., Spanning Tree Protocol (stp), Rapid Spanning Tree Protocol (rstp), or Multiple Spanning Tree Protocol (mstp)
O5	OEM to review vulnerability of any firewalls installed with default configuration or not configured.	Note configuration for downstream users to configure.
O6	OEM to review for vulnerabilities of DNS exfiltration and DNS servers not configured to reject untrusted, unknown, or external hosts. Does not apply to non-DNS components or if the DNS host is disabled.	Identity risk due to misconfigured DNS that may negatively affect OEM system or equipment.
O7	List vulnerabilities that may affect essential services (1/5.1). If none are known, the OEM is to state "No known cybersecurity vulnerabilities affecting essential services are identified at this time".	

Note:
In Item F1, the requirement is to enter each component into the National Institute of Standards and Technology (NIST) National Vulnerability Database (NIST NVD) or other recognized national cybersecurity organization to see if the device, software, or firmware is listed. If listed in NIST NVD, then the OEM is to provide the Common Vulnerability Scoring System (CVSS) score or other score from another recognized database of identified software vulnerabilities. If listed, the OEM is to describe mitigation initiatives implemented, if any. If no mitigation initiatives by the OEM are underway or planned, the OEM is to state, "No mitigation initiatives are planned". APIs, if any, are to be included in the review.
If nothing is listed with the NIST NVD or other organizations, the OEM is to state, "No NIST NVD (or other organization) found on ____(date)."

2.3 Equipment Description Document *(1 August 2023)*

The OEM is to submit a revision-controlled description of the OT functionality of each computer-based system, component, or equipment under consideration for an ABS CyberSafety PDA. The OEM is to include the sub-supplier in the functional description and vulnerability analysis and report. At a minimum, the description is to address the following:

2.3.1 Computer-based System or Component Functional Description *(1 August 2023)*

The functional description may be an operator manual, user manual, or specification detailing the functionality of the computer-based system or component. The items listed below are part of the Vulnerabilities Report.

i) Unique model number or name identifying the computer-based system or component. If the component or computer-based system was previously design assessed, the unique model number or name is to be identical to the previously design assessed computer-based system.

ii) OEM's serial number(s) or equipment tracking identifier of the initial computer-based system.

iii) OT functional description(s) to be submitted:

a) Description of functionality when the system is in a "normal state".

b) Description of functionality when the system is in a "degraded state". May be described in the FMEA, if available. If not available, the OEM is to state, "Degraded state functionality not available".

c) Description of functionality when system has "failed". May be described in the FMEA, if available. If not available, the OEM is to state, "Failed state functionality not available".

d) Overall designation of computer-based system Integrity Level (IL) (see Section 3, Table 1 of the *SQM Guide*) as assigned by the OEM.

e) Systems or components not installed or connected to Primary or Secondary Essential Systems or Category II or III systems:

1) Safety FMEA report, if required by other ABS Rules or Guides. If none required, the OEM is to state, "No FMEA required by ABS Rules or Guides and not installed in nor connected to Primary or Secondary Essential Systems or Category II or III systems".

f) Systems or components installed or connected to Primary or Secondary Essential Systems or Category II or III systems:

1) Safety review analysis for the impact that the failure of the PDA system has upon the Primary or Secondary Essential Systems or Category II or III systems. If there an impact, the OEM is to be an ABS CyberSafety Service Supplier (Section 2) and submit safety analysis to ABS.

g) Connection complexity (Discrete, Simple, Complex, Very Large Network) for OEM scope of work (see 1/5.1).

iv) System-wide time source for computer-based systems or the capability to timestamp security events for components.

v) OEM's computer-based system's software version number(s) at the time of Factory Acceptance Test of the initial system.

vi) OEM's firmware version number for computer-based components implemented at Factory Acceptance Test (FAT) of the initial system.

vii) Controlled Equipment Registry is a list of digitally-enabled components the OEM is supplying for each computer-based system included in the ABS PDA (Manufacturer, Model number):

a) Network infrastructure components (such as switches and routers)

b) Servers detailing Operating System version and Build number

c) Personal Computers detailing Operating System version and Build number

d) PLCs or control system detailing:

1) Operating System version and Build number

2) Firmware version

e) HMIs detailing Operating System version and Build number

f) Wireless access points or routers

g) Other network or computer-based system components, networked, serially or wirelessly connected, digitally-enabled and connected devices to be included in the PDA and supplied by the OEM (IOT, IIOT and COTS)

h) Sub-supplier digitally-enabled components, as information is provided by the sub-suppliers.

viii) Controlled Software Registry is a list of software installed in the digitally-enabled components the OEM is providing. List software installed in sub-components from sub-suppliers, if provided with the version numbers from the Sub-suppliers. The following are to be listed (use "N/A" if not used in the configuration):

a) OEM provided software

b) OEM's required Application Program Interface(s) (APIs)

c) Operating system (build number and version number)

d) Application libraries

e) Firewall(s)

ix) Wireless access point configuration (including but not limited to Wi-Fi, cellular-based broadband, Bluetooth, and RF datalink), if any

x) A listing of enabled or disabled digital services and ports (Ports, Protocols and Services (PPS)). If PPS are project dependent, state, "PPS are project dependent".

2.3.2 Computer-based System's Connections *(1 August 2023)*

i) Describe OEM's cybersecurity measures applied during remote digital connection to the fielded computer-based system:

a) Reference pertinent OEM's cybersecurity policy governance for remote connection.

b) Describe identity controls and verification requirements for authorized access (password length, complexity, etc.) by OEM's personnel from remote locations to client assets.

c) Describe Remote Connections:

1) If no remote (Internet) connection, state, "No remote connection required".

2) Describe how a remote session is terminated, whether remote sessions are designed to time-out automatically and specify time-out criteria.

3) Specify the number of remote concurrent sessions allowed or describe how sessions are limited or controlled.

4) Describe how remotely transferred data is classified and if or how the connection protection is managed – including use of encrypted channels or applications required to protect access to the data transfer operations.

d) Describe monitoring tools (like Security Information and Event Management) or security activities employed for managing unauthorized access detection or protection performed by this computer-based system or component, if any.

e) Describe the process used for performance data and system logs collection and analysis, if any.

f) Describe any intrusion detection or intrusion protection system built into the computer-based system or component, if any.

ii) Describe the number of allowed local concurrent sessions and how sessions are limited or controlled and terminated.

iii) The OEM is to remove any undocumented, development or backdoor access accounts before delivery.

iv) The OEM is to disable any basic web servers unless required for computer-based system operation or the owner. List any known vulnerabilities associated with web servers, if enabled.

2.4 Computer-Based System's Topology Drawing *(1 August 2023)*

The topology drawings are to be revision-controlled and included in the Vulnerabilities Report. The requirements in 3/2.4 do not apply for computer-based systems with a discrete or simple connection. If the OEM's networked system, when installed in its final configuration, has less than 10 connected devices in its network segment, then it is permissible to list the nodes and connected devices in a table that includes the information below. The OEM's computer-based system's network topology drawing(s) is to show connections within the OEM's scope of supply, including:

i) Digitally enabled components, network infrastructure components. The remote Input and Output (I/O) connections may be shown as a single connection regardless of the number of I/O connections.

ii) HMIs and control panels connected to OT network(s)

iii) Sub-supplier's and contracted and known third-party control and IT equipment connected to OEM's OT network(s). If the sub-supplier has a network segmented from the OEM's OT network, show sub-supplier's connection (gateway) to OEM's network.

iv) IT office network connection(s) to the OEM's network. It is permissible to identify only the network port(s) and not identify specific office equipment, unless the equipment is within the OEM's scope of supply.

v) Data collection connection(s). It is permissible to identify only the network port(s) and not identify data collection equipment, unless the equipment is within the OEM's scope of supply.

vi) Satellite and remote access connection. It is permissible to identify only the network port(s) and not identify remote access equipment, unless the equipment is within the OEM's scope of supply.

vii) Wireless connection point(s), if any.

viii) Show cybersecurity functions (routers, programmed switches, etc.) installed.

ix) Network monitoring system installed by the OEM or OEM's sub-supplier.

a) The OEM is to state if network monitoring is installed by the OEM or OEM's sub-supplier.

b) The OEM is not to permanently disable a port to allow for future network monitoring if network switches are within the OEM's scope of supply.

2.5 Anti-malware Scans and Software Backups *(1 August 2023)*

i) The OEM is to perform an anti-malware scan at FAT of every computer-based system and make the results available for ABS review upon request. The expected information, at a minimum, is to denote:

a) Name of vessel or offshore asset

b) Date of the scan

c) Anti-malware software name

d) Virus definition number

e) Scan Report. If the scan reports known code as potential malware, note that it is expected and state the reason.

f) OEM is to identify and report any application specific software that may not be able to be scanned by malware detection.

ii) Malware-free software is to be backed up in a safe location with parameters by OEM or may be provided to the owner. The Surveyor may request to be informed of the location of backed-up software at the audit.

3 Hardware and Software Updates *(1 August 2023)*

The ABS CyberSafety PDA Certificate is associated with described cybersecurity functions or controls and components of the computer-based system. All computer-based systems ordered with an ABS CyberSafety PDA Certificate are to be delivered with components described within the ABS CyberSafety PDA documentation.

- Subsection 3/3 is applicable to the ABS CyberSafety PDA only.
- Refer to Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* for applicable PDA requirements associated with the computer-based system hardware and equipment.

3.1 Updates and Additions to the PDA Defined Computer-Based System *(1 August 2023)*

The installation of newer, more capable, or supportable components with new hardware and software within a computer-based system is anticipated, and minimally requires the submittal of a PDA revision request. These updates may resolve discovered cybersecurity vulnerabilities, fix software bugs, or added functionality. Computer-based system updates are listed below to keep the ABS CyberSafety PDA current for various hardware or software changes or updates to the computer-based system:

i) Additions or changes to the hardware PDA defined computer-based system (3/3.2):

a) The owner or shipyard may require additional computing components to be installed within the boundary of the PDA defined network and the shipyard requires the computer-based system be delivered with ABS CyberSafety PDA.

1) Unless specified by the Owner or shipyard, network infrastructure components may not require a new PDA, just an update to the existing PDA and new Vulnerability Report.

2) As a Recognized CyberSafety Service Supplier, the OEM may either update the PDA or apply for a new PDA.

3) Components and systems connected outside the boundary of the CyberSafety boundary do not affect the PDA and do not require a new or updated PDA.

ii) Hardware replacement:

a) Replacement-in-kind of network architecture component does not require notification of ABS (same manufacturer, same model)

b) Replacement-in-kind of control system component does not require notification of ABS (same manufacturer, same model)

c) Replacement-not-in-kind of computer-based system's digitally-enabled component, HMI, Personal Computer, network infrastructure component, or servers requires a new equipment PDA to be requested and updates or revision to the ABS CyberSafety PDA (see 3/3.3).

iii) Software or firmware updates. See 3/3.3 in all cases for all digitally-enabled components.

3.2 Recognized Service Supplier with Component Additions to a PDA *(1 August 2023)*

The OEM may install additional components (both digitally-enabled process equipment, cybersecurity functions or network infrastructure) connected to the computer-based system's PDA-defined network as required by the specification for a specific vessel, the OEM is to:

i) Update and submit the Vulnerability Report (3/2.1) and reference previous PDA certificate number.

ii) The *Marine Vessel Rules* and ABS *Rules for Conditions of Classification (Part 1)* may apply and have additional requirements.

3.3 Product Design Assessment Software Updates *(1 August 2023)*

The OEM is to submit a description of the software changes to ABS. ABS is to review and determine if the change requires an engineering review.

i) Recognized Service Suppliers are to complete the PDA revision application form at www.eagle.org.

a) OEMs are to submit Section 3 documents (Vulnerability Report) and Type testing report.

SECTION 4

Surveyor Audits and Type Tests for ABS CyberSafety

1 ABS CyberSafety PDA Type Test *(1 August 2023)*

Equipment for an ABS CyberSafety PDA is to be type tested by the OEM for ABS CyberSafety. This type test is to be witnessed by ABS and may be performed on board or at the factory. Type testing per Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification (Part 1)* may also apply to the computer-based system or component.

The ABS CyberSafety PDA has an ABS CyberSafety type test on the first instance of the component or computer-based system and may have other type testing required by the Rules associated with equipment PDA. Unit certification is not required for CyberSafety PDA.

1.1 ABS CyberSafety Type Test *(1 August 2023)*

The ABS CyberSafety type test consists of the following:

i) Digitally-enabled components match the topology drawing and/or Controlled Equipment Registry.

- ***a)*** Items to be verified are:
  - ***1)*** Computer-based System's control system components (PLC, I/O cards, network, etc.)
  - ***2)*** Network equipment (wired and wireless), within the scope of supply.
  - ***3)*** Network infrastructure components, within the scope of supply.

ii) Computer-based system software current version number(s) are displayed with documentation provided to Surveyor.

iii) OEM installed cybersecurity functions (hardware and software) software version number(s) with documentation provided to Surveyor.

iv) Accessible physical ports (USB and RJ45) are indicated to the Surveyor, either on the component or on the drawing, and these ports are blocked or disabled.

v) The OEM is to provide the Surveyor with a current Controlled Software Registry listing.

vi) An ABS Surveyor is to witness the type testing for all IL2 and IL3 assigned computer-based systems. The Type Testing Plan is to be made available to the Surveyor for verification at the time of testing.

2 Manufacturers Affidavit of Compliance (MAoC) *(1 August 2023)*

Manufacturers are required to provide a written affidavit of compliance stating that their products are designed, manufactured, assembled, and tested in accordance with specified codes, standards, or

specifications, and the additional requirements of this Guide, as applicable. The codes, standards, or specifications must be stated in the manufacturer's affidavit of compliance.

i) The manufacturer's affidavits of compliance are to accompany the systems, subsystems, or equipment placed on board and are to be verified by Surveyors prior to final acceptance of the system.

ii) See Appendix 2 for an example of manufacturer's affidavit of compliance and its contents.

3 ABS CyberSafety OEM Audit

3.1 ABS Recognized Service Supplier Initial Audit *(1 August 2023)*

After engineering review is complete and all comments are closed, OEM's who are seeking Service Supplier recognition are to proceed with the audit of the following items:

i) CSO audit finding or reviews [2/2.2.2v)]

ii) CSO corporate technical risk review tolerance and technical risk mitigation evaluation documents [2/2.2.2vi)]

iii) Incident Response Plan including the recovery procedure for the computer-based system under consideration for the ABS CyberSafety PDA [2/2.2.3iv)a)]

iv) Records of tabletop exercises focused on client recovery from a cyber incident for the computer-based system under consideration [2/2.2.3iv)b)]

v) Any changes to cybersecurity policies, procedures, change management and configuration control since the last ABS audit [2/2.2.4]

vi) Demonstrate Change Management and Configuration Control system [2/2.2.7]

vii) Anti-malware scan reports [3/2.5]

viii) Software backup [3/2.5ii)]

3.2 ABS Recognized Service Supplier Annual Audit *(1 August 2023)*

3.2.1 Annual Report

The OEM is to submit to ABS an annual report prior to the annual audit to maintain the Service Supplier Recognition denoting:

i) The number of business-impacting cybersecurity incidents recorded in the past 12 months.

ii) Any change in software development and if there are any changes in using third party programmers.

iii) Percent of software development personnel completing OEM's cybersecurity training.

iv) Confirmation of OEM review of vulnerabilities and security requirements of all ABS CyberSafety PDA systems and components during the year and updates to software and the Vulnerability Report.

v) Number of policies and procedures reviewed and/or updated in the past year.

vi) Reviewed development endpoints to identify and remedy security risks.

a) Endpoints are controlled by multi-factor or password access to the systems and secure physical access to development areas.

b) Review for non-secure network (office, Wi-Fi, Bluetooth) connections. Report and add protective functions if the connection is required.

vii) Additions for Cloud Security holders.

a) Number of ABS CyberSafety PDA systems installed providing data to cloud site.

b) Number of clients utilizing thin clients or applications.

c) List of updates to client's applications in the past 6 months.

d) Added or changed Cloud Provider within the Cloud Security boundary.

e) Added or changed Service Category within the Cloud Security boundary.

3.2.2 Audit

In addition, the OEM is to proceed with the audit in accordance with 4/3.1

4 OEM Service Supplier Annual Report for Vessels with CS-System, CS-1, and CS-2 notations *(1 August 2023)*

An annual report described in 4/4.1 below is to be completed by the OEM and provided to the vessel/unit's owner so that the ABS Surveyor can evaluate the performance of the OEM equipment during the vessel Annual Survey for **CS-System**, **CS-1**, and **CS-2** notations (see the ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Industries – ABS CyberSafety® Volume 2*).

4.1 OEM Service Supplier Annual Report

The OEM's or Current Equipment Manufacturer's (CEM) annual Service Supplier Report is to be provided to the attending Surveyor prior to the Annual Survey. The OEM's inspection is to be done within 3 months of the survey window and is to list:

i) The ABS Service Supplier certificate number.

ii) The copies of ABS PDA for the equipment installed and inspected on board.

iii) Details of software findings, failures, and updates since the last report (such as feature, improvement, failures, and safety and performance issues).

This is for all PDA(s) software findings, whether the finding is related to any software update caused by any condition or improvement. It excludes configuration, parameters, and tuning of systems.

iv) Details of software findings closed since the last report.

v) Details of software findings closed as defined per the OEM's MoC policy.

vi) Any pending resolution of the findings from internal audits.

vii) Any modification/replacement found during the inspection.

SECTION **5**

Requirements for Cloud Security *(1 August 2023)*

1 Cloud Security Introduction

Cloud providers rent server capacity accessible via the Internet. Benefits of using the cloud include on-demand storage, supplied operating system, security, and ability to economically expand capacity. Cloud providers and OEMs each have cybersecurity responsibilities for their respective infrastructure services, applications, and respective client access.

The cloud provider has responsibilities to segregate access and data between its clients. The OEMs similarly segregate access and data between the OEM's clients.

The requirements for Cloud Security do not pertain to the cloud provider's internal cybersecurity policies, procedures, and practices. ABS relies upon the cloud provider's third-party audits and certificates. The Service Level Agreement lists the OEM's responsibilities where ABS derived the Cloud Security requirements. The OEM's cloud needs dictate the responsibilities of both the OEM and the cloud provider, which vary based upon the Service Category that meets the needs of the OEM.

There are three (3) general Service Categories (listed in order of increasing OEM security responsibilities) offered by cloud providers:

1) Software as a Service (SaaS)

2) Platform as a Service (PaaS)

3) Infrastructure as a Service (IaaS)

The OEM has responsibilities to set up and maintain cybersecurity and monitor for changes to operating systems, applications, libraries, etc. The OEM's and the cloud provider's responsibilities are detailed in the Cloud Provider's Service Level Agreement.

To maintain cybersecurity resilience, the OEM is to consider updates in the following:

- Operating systems
- The OEM's runtime software, Application Program Interfaces (APIs)
- Applications (Apps)
- Controls on the OEM's client access and read and/or write privileges to the cloud site

The OEM is responsible for using cybersecurity functions to protect data between clients and for configuring each client's platform and then monitoring security. The cloud provider is to update the infrastructure associated services according to the Service Category and Service Level Agreement.

1.1 ABS Service Supplier Recognition

The ABS Service Supplier Recognition indicates the OEM is committed to maintaining a cybersecure environment. The OEM's responsibilities involve securing OEM's client's access to the cloud, software updates, and disciplined monitoring of logs and security response. The CyberSafety Service Supplier Recognition indicates the OEM's maturity and commitment to maintain a cybersecure environment.

i) The OEM is to be a Recognized ABS CyberSafety Service Supplier or be actively engaged in seeking an ABS CyberSafety Service Supplier recognition [see Section 2].

a) OEM is to obtain the ABS CyberSafety Service Supplier Recognition prior to the Cloud Security endorsement.

ii) A Cloud Security endorsement will not be granted without an ABS CyberSafety Service Supplier Recognition.

iii) A Cloud Security endorsement will be suspended upon an invalid, revoked, or expired ABS CyberSafety Service Supplier Recognition.

iv) The Cloud Security system is to be associated with an ABS CyberSafety PDA computer-based system, component, or equipment that is providing the data to the cloud.

a) The OEM is to submit the associated ABS CyberSafety PDA number for the computer-based system, component, or equipment that is providing the data to the cloud.

2 Requirements Based on Service Category

2.1 Cloud Provider's Audits Reports and Certificates

The cloud provider is to have independent third parties conduct security audits and issue certificates or reports indicating compliance with security requirements. ABS requires compliance with the American Institute of Certified Public Accountants' Service Organization Controls 1, Service Organization Controls 2 or Service Organization Controls 3 cybersecurity reports (SOC1, SOC 2 and SOC 3). Other reports from recognized equivalent organizations may be considered on a case-by-case basis.

The OEM is to submit the following information concerning their cloud provider:

i) Latest available cybersecurity third party audit report summary or certificate; and

ii) Other publicly available quality and cybersecurity certificates (ISO 27001, ISO 9001, etc.)

2.2 Cloud Data Security

The OEM is to protect (i.e., encrypt) the data, secure the access, and segregate the data between OEM's clients. The cloud provider manages activities that may expose the data unless the data is always protected.

i) The OEM is to state if the OEM has a contract provision stating that the cloud provider is to keep the data protected.

ii) The OEM is to:

a) Secure client access to the cloud.

b) Update OEM's software apps, APIs, runtime software, etc., as required.

c) Monitor logs.

iii) The OEM is to state if the cloud provider has access to the encryption key(s).

a) The cloud provider may also be the manager of the encryption keys for the OEM.

iv) The OEM is to state method of data deletion (made unreadable and irretrievable) in the cloud environment.

a) The OEM is to describe end-of-service-life cloud or offline archiving or deletion of data.

3 OEM Requirements Based on Service Category and Service Level Agreement

3.1 Service Categories and Service Level Agreement

3.1.1 Service Categories

Different Service Categories provide the OEM with services offered by the cloud provider. The cloud provider services always include the hardware, overall cybersecurity, virtual machines, and APIs that connect the cloud provider's services to the OEM's software. Based on which Service Category is utilized, the cloud provider may offer the operating system, database(s), and managed connections between rented Service Categories on the same cloud. The OEM may store the data in one category and then link the storage with the client facing applications in another Service Category. The cloud provider is responsible for segregating data between the cloud provider's clients. The general categories are:

- *Software as a Service (SaaS).* The cloud provider hosts the OEM's applications. The OEM is responsible for OEM's software updates, access, and end point control.
- *Platform as a Service (PaaS).* The cloud provider services can range from IaaS to SaaS services. The OEM security responsibilities also vary per the Service Level Agreement.
- *Infrastructure as a Service (IaaS).* The cloud provider hosts the OEM's operating system, database, applications, and APIs. The OEM is responsible for updating and maintaining the software.

3.1.2 Service Level Agreement

The Service Level Agreement is a contract wherein the cloud provider and OEM agree to specific responsibilities and services. Service Level Agreements may prescribe compliance criteria of the Service Level Agreement's terms and conditions.

4 Cloud Security Requirements

Regulatory requirements (such as GDPR and PCI DSS) are beyond ABS's scope. If the OEM desires to submit the audit report to meet ABS requirements, the OEM is to remove or redact information beyond the ABS requirements.

4.1 General ABS Cloud Requirements

The following are applicable regardless of the Service Category rented from the cloud provider.

4.1.1 Cloud Provider's and OEM's Basic Information

OEM is the submit the following:

i) Name of cloud provider.

ii) Name or IP address of the OEM's website where OEM's clients connect.

iii) List Service Category or Categories the OEM is renting from the cloud provider (IaaS, PaaS, SaaS). If more than one, list the relationship of the Service Categories.

Example: Database is located on the IaaS and OEM's client connects to the SaaS with dedicated links to pass data per the client's request.

iv) If the OEM is renting Platform as a Service (PaaS), the OEM is to describe the services.

v) Service Level Agreement(s).

vi) Authentication and management process used for clients. The OEM is to utilize OAuth 2.0 or higher or other listed below for client's protocol for authorization:

a) OAuth 2.0 or higher.

b) OpenID (Connect OpenID Foundation).

c) UMA 2.0 (Kantara Initiative).

d) IndieAuth (World Wide Web Consortium).

e) Other (OEM to define and provide reference source).

4.1.2 Access Requirements

The OEM is to submit the following to ABS:

i) *OEM's Clients Access Requirements.* The minimum OEM's client access requirements are:

a) State the required minimum length of password (minimum number of characters).

b) The OEM is to require at least one number.

c) The OEM is to require at least one special character.

d) Password lifetime is to be less than or equal to 90 days.

e) Multi-factor authentication is required to renew passwords.

f) OEM is to state if Single Sign-On is to be allowed.

ii) *OEM's Administrator Access Requirements.* The minimum OEM's administrator access requirements are listed below:

a) State the required length of password (minimum number of characters).

b) At least one number is required.

c) At least one special character is required.

d) Password lifetime is to be less than or equal to 90 days.

e) OEM to state if Single Sign On is allowed as the IaaS or PaaS administrator.

f) OEM to state if a Bastion Host is used for administrator purposes.

4.1.3 Cloud and OEM Server and Runtime Logs

The cloud provider offers various logs depending upon the OEM selected Service Category. The OEM selects which events to monitor from the available logs. Cloud providers may provide automated monitoring and email alarms for the selected events from the logs.

i) The logs are to be retained for six (6) months.

ii) The OEM is to select the logs and events or parameters to monitor (Cloud Provider & OEM logs).

iii) The OEM is to submit the following:

Notes:

- The OEM is to review available cloud provider logs listed below monthly (alarmed logs are the same as being monitored and have no requirement for a monthly review).
- If the cloud provider did not make a log available to the OEM, the OEM is to state, "Not Available".

a) Logs to be reviewed for Software as a Service (SaaS) and Platform as a Service (PaaS) Service Categories:

- Admin
- Client access
- Webserver

- Cloud provider's software (application and APIs)
- Database
- Malware
- Firewall (network and/or server)
- State other logs being monitored or alarmed

b) OEM is to list other available security logs being monitored

c) Logs to be reviewed for Infrastructure as a Service (IaaS) Category:

SaaS and PaaS logs (as described above)

- Hypervisor
- Management Console logs, as allowed by cloud provider
- Virtual Machine Manager
- Operating System security
- Administrator access

iv) The OEM is to submit logs pertaining to OEM's client access, OEM supplied applications, runtime software and security. OEM to list name of logs monitored.

v) The OEM is to maintain a record of the monthly log reviews.

4.2 Client Access Software

4.2.1 Client Software

i) The OEM is to state if the OEM's clients use thin client software to access the cloud or an OEM supplied application.

a) Include all devices (phones, tables, PCs)

ii) The OEM is to state if equivalent (nearly the same) application software is installed for most to all of the OEM's clients.

4.3 Software Updates

4.3.1 Cloud Provider Software Updates

i) The OEM is to submit copies of notification(s) from the cloud provider for software updates in the past 6 months. If none, the OEM is the state, "No cloud provider software updates".

4.3.2 OEM Software Updates

i) The OEM is to submit copies of notification(s) sent to clients for software updates in the past 6 months. If none, the OEM is the state, "No OEM software updates".

a) Includes applications and runtime software located on the cloud and client-located applications on any client devices.

5 Encryption Key Management

Encryption key management provides security between the OEM's clients and the cloud provider's other clients. The cloud provider's other clients are the responsibility of the cloud provider. Management of the keys may be by the cloud provider or by the OEM depending upon the Service Level Agreement.

i) The OEM is to state which organization (OEM or cloud provider) manages the encryption keys for the OEM's clients.

6 Surveyor Audits

Cloud Security does not require a Type Test.

6.1 Audit Additions for Cloud Security Endorsement Holders or those Seeking the Cloud Security Endorsement

In addition to the items in 4/3.1, the ABS Surveyor is to verify the following:

i) OEM's review of logs has occurred for:

- *a)* OEM Administrator
- *b)* Client access
- *c)* Cloud provider
- *d)* Application events

Note: If logs are monitored and alarmed, verify emails sent for alarms.

ii) Software updates

- *a)* Notifications from Cloud provider for updates, if any, in the last 6 months
- *b)* Notifications from OEM to clients for updates, if any, in the last 6 months

APPENDIX 1

Check List for OEM Company and Equipment for ABS CyberSafety

1 OEM Service Supplier Recognition Check List *(1 August 2023)*

Appendix 1, Table 1 contains the requirements and references for an OEM seeking to be registered as a Service Supplier.

TABLE 1
OEM Company Requirements for Service Supplier Check List *(1 August 2023)*

Reference	*Requirement*
2/2.2.1	OEM to state foundational cybersecurity standard used by OEM
2/2.2.2	**Cyber Security Office (CSO)**
2/2.2.2i)	Mission statement of CSO and goals for the computer-based systems
2/2.2.2ii)	Name or titles of the CSO members
2/2.2.2iii)	Roles and responsibilities of CSO members, including approvals and authorities
2/2.2.2iv)	OEM's organizational chart showing the CSO
2/2.2.2v)	Upon request: CSO audit records
2/2.2.2vi)	Upon request: Corporate technical risk tolerance and technical risk evaluation documentation
2/2.2.3	**OEM's Incident Response Team Organization (IRT)**
2/2.2.3i)	Organization, office, or persons who are responsible for providing support to clients who require assistance to recover form a cyber-related software failure
2/2.2.3ii)	Incident Response Plant with recovery procedure
2/2.2.3iii)a)	OEM to submit: Incident Response Policy and procedure
2/2.2.3iii)b)	OEM to submit: Mission statement of the IRT
2/2.2.3iii)c)	OEM to submit: Roles and responsibilities of IRT members, including approvals and authorities
2/2.2.3iv)a)	Upon request: Incident Response Plan for the computer-based system
2/2.2.3iv)b)	Upon request: Indication of periodically performing tabletop exercises focused on client recovery from a cyber incident
2/2.2.3iv)c)	Upon request: Finding of any incident response investigation of a reported computer-based system failure, with approved remedies and implementation timeline, or the procedure for such investigation
2/2.2.4	**OEM's Cybersecurity Policies and Procedures**

Reference	*Requirement*
2/2.2.4i)a)	Physical and access security
2/2.2.4i)b)	Acceptable use policy of OEM's digital devices, including portable devices
2/2.2.4i)c)	Digital access, registration, and de-registration of OEM's personnel and contractors
2/2.2.4i)d)	Protection of information (during processing, storage, and data breach response)
2/2.2.4ii)a)	Remote access (into OEM's network)
2/2.2.4ii)b)	Use of wireless and mobile devices
2/2.2.5	**OEM's Internal Risk Management**
2/2.2.5i)	If not ISO 27001 Certified and upon request: Enterprise and product cyber risk assessment policies and procedures
2/2.2.5ii)	If not ISO 27001 Certified and upon request: Documents describing periodic cyber risk assessment of enterprise business systems with consideration of controls in place to manage identified risks
2/2.2.5iii)	Upon request: Documents describing periodic technical cyber risk assessments of products, including risks identified, risks tolerated or accepted, controls embedded in products to manage identified risks, and controls recommended for managing risks after product implementation.
2/2.2.6	**Cybersecurity Training**
2/2.2.6i)a)	Cybersecurity awareness and training topics
2/2.2.6i)b)	Titles of provided training topics and titles of personnel who periodically receive the training
2/2.2.6i)c)	Records of logs of completions of training by personnel and contractors
2/2.2.6i)d)	On-boarding cybersecurity training topics for new personnel (if different from above)
2/2.2.6i)e)	Schedule of periodic refresher cybersecurity and change management policies and procedure training
2/2.2.7	**OEM Change Management and Configuration Control**
2/2.2.7i)	Change Management policy and/or procedure
2/2.2.7ii)	Tracking of change management from request through implementation
2/2.2.7iii)	Software change management program or practices to manage inherent evolutionary conditions
2/2.2.8	**Third Party Involvement in Programming of the OEM's Software**
2/2.2.8i)	State if the third party uses the same policies and procedures as the OEM
2/2.2.8ii)	Submit the 2/2.2.1 through 2/2.2.7 documents if the documents are different from the OEM
2/2.2.8iii)	OEM to detail how the OEM receives, verifies, and tests software obtained from third parties
2/2.3	**Copies of Certificates**
2/2.3	Copies of ISO-9001, ISO-27001, ISA-62443, or other cybersecurity certificates

2 Equipment Level Requirements Check List *(1 August 2023)*

Appendix 1, Table 2 contains the requirements and references for equipment for the ABS CyberSafety PDA.

Appendix 1, Table 3 contains the requirements and references for the Cloud Security endorsement.

TABLE 2
Equipment Level Requirements for ABS CyberSafety PDA Check List
(1 August 2023)

Reference	*Requirement*
3/2.1	**Vulnerability Report**
3/2.1i)a)	Vulnerability Analysis (see 3/2.2)
3/2.1i)b)	Description of known OEM cybersecurity vulnerabilities that are not mitigated by the OEM cybersecurity functions
3/2.1i)c)	OEM installed cybersecurity functions (hardware and software)
3/2.1i)d)	OEM login requirements to OEM equipment and cybersecurity functions
3/2.1i)e)	Computer-based system or component description documents (normal state – required, degraded and failed states – if available) (see 3/2.3)
3/2.1i)f)	Sub-supplier functionality description, vulnerabilities description, and topology drawings as reported by sub-supplier, if any
3/2.1i)g)	Sub-supplier remote connection vulnerabilities, as reported by sub-supplier, if any
3/2.1i)h)	OEM's topology drawing (see 3/2.4)

TABLE 3
Cloud Security Endorsement Check List *(1 August 2023)*

Reference	*Requirement*
5/1.1	The OEM is to be a Recognized ABS CyberSafety Service Supplier or be actively engaged in seeking the recognition. The OEM must earn the recognition prior to ABS awarding the Cloud Security endorsement.
5/2.1i)	Latest cloud provider's security third party audit report summary
5/2.1ii)	Publicly available quality and cybersecurity certificates (ISO 27001, ISO 9001, etc.)
5/2.2i)	OEM is to state if the client has a contract provision with the cloud provider to keep the data protected
5/2.2ii)	OEM is to secure client access to cloud, update OEM's software apps, APIs, etc., monitor logs
5/2.2iii)	OEM is to state if the cloud provider has access to the storage data's encryption key
5/2.2iv)	OEM is to describe how cloud data is deleted (make unreadable and irretrievable) in the cloud environment
5/2.2iv)a)	OEM is to describe end-of-service-life cloud or offline archiving or deletion of data
5/4.1.1i), ii), iii)	OEM is to submit the following: • Name of the cloud provider • Name or IP address of the OEM's website where the OEM's clients connect • List of Service Category or Categories the OEM is renting
5/4.1.1iv)	If the OEM is renting PaaS, the OEM is to describe the services
5/4.1.1v)	OEM is to submit the cloud provider Service Level Agreement

Reference	*Requirement*
5/4.1.1vi)	OEM is to submit which authentication and management process is used for clients
5/4.1.2i)	OEM is to submit client access requirements
5/4.1.2ii)	OEM is to submit OEM's administrator access requirements
5/4.1.3	OEM is to submit the names of the logs (cloud provider and OEM logs) monitored or alarmed
5/4.1.3iii)	OEM is to review available cloud provider logs
5/4.1.3iii)a)	Logs to be reviewed for SaaS and PaaS
5/4.1.3iii)b)	OEM is to list other available security logs being monitored
5/4.1.3iii)c)	Logs to be reviewed for IaaS
5/4.1.3iv)	OEM is to submit logs pertaining to OEM's client access, OEM supplied applications, runtime software and security
5/4.1.3v)	OEM is to maintain a record of the monthly log reviews
5/4.2.1i)	OEM is to state if the OEM's clients use a thin client application software
5/4.2.1ii)	OEM is to state if the equivalent application software is installed for most to all OEM's clients
5/4.3.1	Cloud provider software update notifications from the past 6 months, if any. If none, state "No cloud provider software updates"
5/4.3.2	OEM is to submit software update notifications sent to clients from the past 6 months, if any. If none, state "No OEM software updates"
5/5	OEM is to state who manages the encryption keys for the OEM's clients (OEM, cloud provider or other)

APPENDIX **2**

Example of Manufacturer's Affidavit of Compliance (MAoC) *(1 August 2023)*

XYZ Software Company

12345 Street Avenue
City, State, [Zip Code/Postal Code]
Country

Date: Jan 01, 2023

MANUFACTURER'S AFFIDAVIT OF COMPLIANCE

Manufacturer & Address: XYZ Software Company
12345 Street Avenue
City, State (Zip Code)

Customer & Address: XYZ Corporation
12345 Street Avenue
City, State (Zip Code)

Customer PO#: AAA-12345

Product Name:

Product Version:

Product Serial Number: XXX-YYY

ABS CyberSafety PDA Number: 22-HS1234567-PDA

Date of Creation:

Code(s), Standard(s) or Specification(s) Applied: (list all applicable)

This affidavit is prepared by the undersigned, authorized representative of the manufacturer, to certify that the product described above and supplied for this order is in full compliance with respect to the design, assembly, and testing in accordance with the referenced code(s), standard(s) or specification(s), and is suitable for the intended use in accordance with the referenced design parameters.

This affidavit is prepared by the undersigned, authorized representative of the manufacturer, to certify that the product described above is in compliance with the requirements of the ABS *Guide for CyberSafety for Equipment Manufacturers, ABS CyberSafety® Volume 7* and is enclosed as part of the product delivery/shipment documents.

Signature
Name :
Title :
Date :