Guidelines on
Maritime Cyber Safety

2018

IRCLASS
Indian Register of Shipping

Guidelines

Maritime Cyber Safety

2018

Contents

Sections

1. General

1.1 Purpose, General Principles
1.2 Surveys
1.3 Definitions

2. Cyber Safety

2.1 Cyber Threats
2.2 Consequences of Threats
2.3 Cyber Risk Management Philosophy
2.4 Implementation Levels and Associated Notations

3. Informed Cyber Safety

3.1 General
3.2 Governance, Policies and Procedures
3.3 Asset Management
3.4 Risk Assessment
3.5 Physical and System Access Control
3.6 Network Security
3.7 System Security Controls
3.8 Detection Controls
3.9 Response and Recovery Procedures
3.10 Training, Awareness and Information Sharing
3.11 Cyber Safety Process Review

Annex I Guidance for Application of Requirements to IT Systems and Control systems

4. Advanced Cyber Safety

4.1 General
4.2 Governance, Policies and Procedures
4.3 Asset Management
4.4 Risk Assessment
4.5 Physical and System Access Control
4.6 Network Security
4.7 System Security Controls

4.8 Detection Controls
4.9 Response and Recovery Procedures
4.10 Training, awareness and information sharing
4.11 Cyber Safety Process Review

Annex II Guidance for Application of Requirements to IT systems and Control systems

References

Section 1

General

1.1 Purpose, General Principles

1.1.1 These Guidelines are intended to provide requirements for evaluating and managing the Cyber Risk of Ships. Ships complying with the requirements as specified in these Guidelines would be assigned additional class notations as indicated in Section 2. For the purpose of these Guidelines, Ship includes mobile offshore units. If requested by the Owner, IRS can verify and certify the associated shore based support facilities, as indicated in Section 2 of these Guidelines.

1.1.2 The intent of these guidelines is to provide a frame work by which an organization can implement a Cyber safety programme on board a ship. The guidelines are not meant to address every possible contingency on ship.

1.1.3 In general, the provisions and principles of Part 1, Chapter 1 of the *Rules and Regulations for the Construction and Classification of Steel Ships* are applicable.

1.2 Surveys

1.2.1 Ships would be subjected to initial surveys for classification and annual surveys. Surveys for assignment of cyber safety notations (See Section 2) would include examination of control system configurations, networked systems and review of documentation, organizational capabilities and procedures.

1.2.2 *Surveys during Construction*. Design checks and verifications would be conducted by IRS surveyors, so that the cyber safety principles are integrated and that these surveys are conducted in consonance with other conventional surveys.

1.2.3 *Surveys after Construction*. The regular survey process (i.e. annual, intermediate and special surveys) would be supplemented by cyber safety assessments, as required. Annual surveys would include checks of the documentation, as indicated in Section 2.

1.2.4 *Occasional Surveys*. Ships may also be surveyed when there are major equipment changes; or cyber-enabled, safety-related networked system configuration changes; or occurrence of cyber-security events. Such Surveys would be conducted based on requests from the Owners.

1.2.5 All surveys for certification to these requirements will be harmonized to the extent feasible and possible with IRS classification survey cycles.

1.2.6 In the context of cyber safety, the certification indicates that at the time of assessment, the organization has established and implemented a cyber security management system in accordance with the requirements of these Guidelines and the surveys, tests and assessments for the cyber-risk profiles and conditions were completed satisfactorily. The continuance of certification or any notation is conditional upon the ship's continued compliance with the requirements of these Guidelines.

1.2.7 *Change of Ownership*. Upon change of ownership, IRS reserves the right to perform out-of-cycle reassessments to verify that the notation remains current under the new organization, when request is made by new owner for continuation of Cyber Safe Notation.

1.3 Definitions

1.3.1 ***Access Control***: is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

1.3.2 ***Antivirus software****:* A computer program designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected files, cleaning infected files or systems, or informing the user that an infected program was detected.

1.3.3 ***Asset****:* means any data, computer or device. Asset management is the control of any data, computer or device.

1.3.4 ***Cyber-attack****:* An attack that involves the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.

1.3.5 ***Cyber-event***: An observable event in a computer network or system resource, which may or may not have consequences.

1.3.6 ***Cyber-Incident***: Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete or render unavailable any computer network or system resource.

1.3.7 ***Cyber System****:* Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.

1.3.8 ***Cyber Safety****:* Cyber safety is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment of a ship. Cyber safety onboard ships protect:

- the operational technology against the unintended consequences of a cyber-incident;
- information and communications systems and the information contained therein from damage, unauthorized use or modification, or exploitation; and/or;
- against interception of information when communicating and using the internet.

1.3.9 ***Denial of Service (DOS)****:* The prevention of authorized access to resources or the delaying of time-critical operations.

1.3.10 ***Denial of Service Attack***: A form of cyber-attack which prevents legitimate and authorized users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack involves a cyber-attacker taking control of multiple computers and/or servers to deliver a denial of service attack.

1.3.11 ***Firewall****:* Firewall is a logical or physical break designed to prevent unauthorized access to IT infrastructure and information.

1.3.12 ***Hacker****:* Most commonly used as a pejorative by the mass media to refer to a person who engages in illegal computer trespass, which is its original meaning, but it can also refer to people engaged in ethical hacking, to the members of the open source and free software community or to home computer hobbyists

1.3.13 ***Information Security***: is the security applied to information (rather than systems) protecting it from unauthorized access, disclosure, modification or destruction.

1.3.14 ***Information Technology (IT)***: The application of science to the processing of data according to programmed instructions in order to derive results. In the widest sense, IT includes all information and all technology; in a much narrower sense, telecommunications technology is excluded - or for some particular reason needs to be emphasized.

1.3.15 ***Intrusion Detection System (IDS)***: is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. Intrusion detection systems (IDS) provide real-time monitoring of network traffic. An IDS can detect a wide range of hostile attack signatures (patterns), generate alarms to alert operations staff and, in some cases, cause routers to terminate communications from hostile sources.

1.3.16 ***Intrusion Prevention Systems (IPSs)***: also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity.

1.3.17 ***Malware****:* Software designed to infiltrate or damage a computer system without the owner's informed consent

1.3.18 ***Operational Technology (OT)***: A hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. It includes devices, sensors, software and associated networking that monitor and control onboard systems.

1.3.19 ***Organization***: Organization means ship owner / manager / bare boat charterer of ship / offshore installation (For the purpose of these Guidelines).

1.3.20 ***Penetration Testing***: A penetration test, commonly referred as 'pen test', is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.

1.3.21 ***Phishing***: A technique used to trick computer users into revealing personal or financial information. A common online phishing scam starts with an e-mail message that appears to come from a trusted source but actually directs recipients to provide information to a fraudulent Web site.

1.3.22 ***Ransomware***: A type of malicious software designed to block access to a computer system until a sum of money is paid. Some forms of ransomware encrypt files on the system's hard drive (a.k.a. crypto-viral extortion), while some may simply lock the system and display messages intended to coax the user into paying.

1.3.23 ***Recovery Planning***: The development and implementation of plans, processes, and procedures for recovery and full restoration in a timely manner, of any capabilities or services that are impaired due to a cyber-event.

1.3.24 ***Router***: A device that sends, or routes, information between two networks (for example, between a home network and the Internet).

1.3.25 ***Social Engineering***: The practice of penetrating system security by tricking individuals into divulging passwords and information about network vulnerabilities. Often done by calling the individual on phone and pretending to be another employee of organization with a computer-related question.

1.3.26 ***Spyware****:* A program that collects information, such as the web sites a user visits, without adequate consent. Installation may be without prominent notice or without the user's knowledge.

1.3.27 ***Virtual Local Area Network VLAN***: A logical grouping of hosts on one or more local area networks (LANs) that allows communication to occur between hosts as if they were on the same physical LAN.

1.3.28 ***Virus****:* Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

1.3.29 ***Worm***: Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial of service attack.

Section 2

Cyber Safety

2.1 Cyber Threats

2.1.1 Cyber threats may originate from multiple sources. Cyber safety assessment is to be carried out considering both internal and external sources of threats. Following sources of threat as a minimum are to be considered as applicable to the system:

- Worms
- Viruses
- Malware
- Unauthorized accesses to sensitive data/control
- Human Errors (inadvertent operations)

2.1.2 In evaluating a cyber-risk the possibility of cyber-attack from the following routes (as applicable for the system), are to be considered as a minimum:

- USB or removable media
- Connection of crew or maintenance laptop, mobile device
- Wi-Fi connection
- Through smart phones
- Physical interference with system

2.2 Consequences of Threats

2.2.1 The consequence of each threat is to be analyzed and documented. The impact of each threat on a particular system and subsequently, in the vessel functions is to be analyzed and identified. The associated risk is to be classified.

2.2.2 The consequences of threats for following conditions as applicable, are to be considered:

- Loss of network
- Loss of connectivity between various parts of control systems
- Gaining unauthorized access to control and IT systems
- Unauthorized change of critical system parameters
- Environmental Impact
- Safety Impact
- Effect on critical application / assignment of the ship

2.3 Cyber Risk Management Philosophy

2.3.1. A five functional approach as indicated by IMO guidelines on cyber risk management and in subsequent sections of these Guidelines is to be adopted.

2.3.2 The five functions which form the basis for Cyber risk management are as follows:

a. *Identify*: Typical assets which are vulnerable to attacks, risks, policies and procedures

b. *Protect*: Systems and procedures such as training, technical protection, controls etc.

c. *Detect*: Systems and procedures to detect a Cyber incident like intrusion detection systems, analyzing anomalies etc.

d. *Respond:* The policies and procedures of the organization to respond to a cyber-incident. For e.g. communication, response planning etc.

e. *Recover*: organization policies and procedures for recovery of critical data, backup philosophy etc.

2.3.3 Various activities encompassing the above functional elements are indicated in further sections along with requirements that need to be complied by the ship, towards an effective management of maritime cyber risk.

2.4 Implementation Levels and Associated Notations

2.4.1 These Guidelines specify broad requirements for two levels of implementation of Cyber Safety and assignment of optional additional notations. These are as follows:

a) **Informed Cyber Safety**, **CyS-I**
b) **Advanced Cyber Safety**, **CyS-II**

2.4.2 The requirements for each tier / notation increase progressively from informed level to advanced level. A brief comparison of the requirements for the cyber safety notations is given in Table 2.4.2. The Ship would be surveyed by IRS for compliance with the requirements of the requested level of cyber safety and the notation would be accordingly assigned based on successful completion of the survey.

Table 2.4.2 : Requirements for Cyber Safety Notations		
DOMAIN	**CyS-I**	**CyS-II**
Governance, policies and procedures	Cyber safety policy, roles & responsibilities	Internal verification of policies and procedures , consider externa issues
Asset Management	Inventory of essential assets hardware, software network, configuration, maintenance	Asset Change, patch management
Risk assessment	Identify threats , vulnerabilities	Vulnerability scan results, penetration test , new threats considered
Physical and system Access control	Physical assess control, system access controls , Remote access	Advanced authentication controls for e.g. bio metric controls, remote session controls
Network Security	Perimeter defense (firewall)	VLANS, VPN ,IDS,IPS, mobile and wireless security
System Security Controls	Malware protection	Data security, information protection process, cryptography
Detection Controls	IDS , event Logs	Anomalies detection, cyber safety centre. Security information and event management (SIEM)
Respond and Recovery procedures	Backups, event reporting.	Recovery plan. Communication. Incident Analysis , forensic analysis External coordination
Training , awareness and information sharing	Basic awareness, sharing of cyber information through internal mails	Detailed cyber security training, Assimilate cyber safety information from Industry expert training
Cyber safety Process Review	Review after change in asset, process	Periodic review of process, new threats , assets, evolving technology

(a) **Informed Cyber Safety**

The organization is to assess the issues related to cyber safety, cyber risks and have documented policies. Controls and procedures are to be in place, to mitigate risks. On-board senior personnel are to be aware of cyber risks. Cyber information is to be shared in informal manner, except in critical situations. The organization implements minimum cyber safety practices. The risks and procedures are to be reviewed whenever there is a change in asset.

(b) **Advanced Cyber Safety**

The policies and procedures are to be reviewed periodically. Specific training is to be imparted to personnel. Detection and protection logs are to be analyzed. The risks and procedures are to be reviewed periodically. All information is to be shared in a formal manner including sharing of information with external bodies. A procedure is to be implemented for continual improvement of cyber safety procedures, risks and controls based on evolving technologies and threat perception

2.4.3 If requested by the Owners of the ship which has been assigned Cyber Safe Notation, shore based facilities may also be assessed for Cyber Safety based on the IRS Guidelines on '*Cyber Safety Guidelines for Land Installations'*. In such cases, the **CyS** notation would be annotated by a qualifier '**+**'. The notation would thereby reflect as **CyS-I +**, or **CyS-II+**, as applicable. For a company having a fleet of ships with varying cyber safety notations, the shore based facilities as a minimum have to meet corresponding requirements specified for the highest notation level of a ship in the company fleet classed with IRS and certified for Cyber Safety Notation.

2.4.4 Documentation

2.4.4.1 Cyber safety documents (as applicable for each level) broadly covering the following are to be submitted (Details are to include both IT and OT systems where applicable):

Cyber Safety Management plan:

Following information / details are to be indicated in the document:

- Brief description of various safety critical equipment / systems;
- Policies and procedures towards Cyber Safety including scope
- Roles and responsibilities of key personnel;
- Risk acceptance and assessment methodology
- Risk Assessment Report;
- Risk register including risk tolerance and risk management philosophy
- Vulnerability analysis (to include systems which are required for all intended operations of the vessel/shore support facility including systems required for environment safety and human safety, business continuity);
- Process for third party risk assessment
- System for sharing cyber safety information.
- Process Review methodology

Cyber Safety Implementation plan:

The plan is to incorporate following details as applicable:

- Operations and Maintenance (O&M) Plan;
- Control system and information system equipment registry;
- Software Registry including registry of software updates;
- Vulnerability test reports, where specified;
- Hardware registry including details of any changes

- Record of cyber incidents and analysis of event logs where applicable
- Details of remote logins
- Software Configuration Management Plan, Policy and Process
- Network diagrams for IT and OT systems
- Functional descriptions of vulnerable software and hardware assets
- Interface /integration diagrams of vulnerable assets
- Test procedures and test records for every change in software and hardware assets for both IT and OT systems.

2.4.5 Documentation requirements indicated above may be reviewed on the basis of identical installations or commonality across ships. The owner is to provide evidence of verifiable similarity among ships of specific types. Similarity includes not just type design (ships of a series), but also similarity of control system construction and implementation. However, onboard verification of all ship systems would be required for each installation.

2.4.6 Cyber system peripherals and network components are to comply with relevant National/ International standards. In an existing ship where evidence to such compliance cannot be demonstrated, the installed equipment may be accepted based on functional tests.

2.4.7 Compliance requirements for each tier/ level of cyber risk management are detailed in subsequent sections.

2.4.8 Each server essential for safety, navigation, communication and control of essential systems are to be powered from two independent sources of power supply. In addition to the above requirement, the systems are to be powered from UPS with at least 15 minutes' backup.

2.4.9 Depending on criticality of the equipment and the risk analysis, additional enhanced controls as specified in IEC 62443, ISO 27001 standards may be required to be provided to meet higher safety levels.

Section 3

Informed Cyber Safety

3.1 General

3.1.1 The requirements indicated in this section along with applicable requirements specified at Section 2 are to be complied with, for assignment of Informed Cyber Safety (**CyS-I**) notation.

3.2 Governance, Polices & Procedures

3.2.1 Cyber Safety Policy

3.2.1.1 Policies and procedures towards implementation of a cyber-safety management system are to be defined. A Cyber safety policy is to be established, implemented and maintained.

3.2.1.2 There is to be a general awareness of cyber risk at senior management level. Senior management at ship level means, Master and Chief Engineer.

3.2.2 Ship Cyber Safety Officer

3.2.2.1 A Ship Cyber Safety Officer (SCSO) is to be identified and nominated. The main responsibilities of the SCSO are to include implementation of the approved cyber safety program and monitoring the effectiveness of the same. As shore support is important for implementation of Cyber safety on board a vessel, the company is to designate a company shore based Cyber security officer. The Ship Cyber security officer is to be supported by Company Cyber security officer for providing on shore support on Cyber safety issues.

3.2.3 Guidelines and Standards

3.2.3.1 In formulating and implementing the Cyber safety requirements following standards/ guidelines may be referred:

- IMO guidelines on cyber risk management
- ISO/ IEC 27001 Standard on Information technology – Security techniques
- ISO/ IEC 27032-Information Technology – Security Techniques - Guidelines for Cyber security
- ISO 31000 – Risk Management-Principles and Guidelines
- IEC 62443 series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems

3.2.4 Internal Context

3.2.4.1 Internal context is the organizational environment in which the cyber safety measures aim to achieve its objectives. Internal context can include an organization's approach to governance, its contractual relationships with customers and its interested parties.

3.2.5 Procedures and processes to carry out risk assessment of ship's IT and OT systems are to be documented. The Risk management practices are to be formally approved and documented.

3.2.6 The organization is to identify and implement a back-up plan for the ship critical systems. The roles and responsibilities during of all the personnel operating the IT and OT systems are to be clearly defined.

3.3 Asset Management

3.3.1 The organization is to identify various processes required for its operations and make a detailed inventory of all information technology (IT) and operational technology (OT) systems required for essential services.

3.3.2 The inventory of assets is to include identification of application software, operating system software and various types of network communications in main and sub systems.
3.3.3 Request for asset changes are to be approved and documented.

3.3.4 Where the version number/ model number of the asset under replacement is different from the installed asset, the configuration of the new asset to meet the desired functional requirements, is to be evaluated prior to installation.

3.3.5 Maintenance and repair of organizational assets is to be performed in a timely manner using approved and controlled tools. The maintenance activities are to be logged.

3.3.6 Remote maintenance of organizational assets is to be approved, logged, and performed in a manner that prevents unauthorized access.

3.3.7 All the communication paths are to be identified and are to be mapped.

3.3.8 All cyber physical systems and software are to be prioritized in accordance with the criticality of the operation they support. Critical areas and corresponding control measures are to be implemented accordingly.

3.4 Risk Assessment

3.4.1 A detailed risk assessment is to be carried out before implementing normal protection devices such as fire walls, antivirus etc. The risk assessment is to be carried out to assess the safety, environmental effects and business risks due to cyber-attack. The results of risk assessment are to be used to

ensure that appropriate measures are selected and the systems are protected in proportion to the risk.

3.4.2 The Risk assessment and analysis is to be carried out to arrive at risk value for an identified vulnerable system. ISO 31000 or equivalent standard may be referred for the risk analysis.

3.4.3 The risk assessment process is to have methods to prioritize the vulnerabilities. The results of physical, health safety and environment (HSE) and cyber safety risk assessments are to be integrated to arrive at overall risk.

3.4.4 Vulnerability assessments of critical systems and potential threats that the ship can face are to be documented. The process involves identification of all systems which when attacked, can result in partial or full compromise of the ship's safety and/ or its impact on environment.

3.4.5 A list of typical onboard vulnerable systems on a Ship is indicated below. The list is indicative and exact list would depend on the type of vessel and its operational requirements:

- Cargo management systems
- Bridge systems
- Propulsion Control system
- Machinery Control system
- Power control systems
- Watertight door systems
- Passenger servicing systems
- Fixed or wireless networks connected to the internet installed on board for the benefit of passengers
- Administrative and crew welfare systems
- Communication systems.

3.4.6 The vulnerability of each system is to be assessed by considering potential routes for misuse or exploitation including the consequences of attack on vessel safety, personnel, the marine environment and loss of vital data. Consequence analysis is to be carried out for each system in the event of failure, misuse, or exploitation.

3.4.7 Following possible sources of vulnerability are to be considered during vulnerability assessment, as a minimum:

- Policies and procedures
- Configuration procedures
- Maintenance procedures
- Software development
- Network communication

3.4.8 A risk matrix is to be prepared where each threat on a particular system and its consequence on personnel safety, vessel operations, vessel safety and environment safety is identified. Risks may be graded based on the severity of consequences. Ex. High, Medium or low.

Guidance note: Risk matrix

a) Impact value – It is a qualitative value assigned to describe the extent of impact to ship when a threat scenario and resulting impact is realized. The impacts can be assigned a number in 1 to 10 or alternatively can be classified as High, medium and low based on the severity of the impact. This value can form the basis for determining which risks are needed to be mitigated immediately. Due to lack of sufficient published risk data on industrial control systems, the qualitative procedures are generally applied.

b) Depending on the severity of risk; a decision is to be made during risk analysis to accept the risk or mitigate the risk. Risks that are accepted should have little to low impact. Risks that are to be mitigated are those that typically have a medium to high impact on ship. Deferring a risk is not recommended, as it would require a detailed assessment of the consequence. The organization can define the required security level based on the risk assessment. The purpose of defining the security levels should be to identify and implement required level of security controls for a given system, based on risk assessment.

c) In selecting a technical control for a particular operational technology (OT) system, the effectiveness of the control to deal with attack for the system under consideration is to be ascertained. For effective operation the confidentiality, integrity and availability (CIA) of the information is to be ensured.

d) For IT systems, the order of importance for an information would be confidentiality, integrity and availability. However, for a control system, the order of importance would be availability followed by integrity and confidentiality.

3.4.9 Both internal and external threats are to be considered.

3.4.10 Cyber incidents are to be classified based on their impact on ship and impact of incidents is to be considered during risk assessment.

3.4.11 The organization is to determine and document its risk tolerance as a basis for creation of policy and risk management activities.

3.4.12 The risk assessment document is to address the following requirements, as a minimum:

- Established risk acceptance criterion
- Identification and documentation of consequences of each threat on vulnerable system
- Approved and documented risk methodology
- Identification of risk priorities based on severity of impact
- Risk classification
- Identify risks which can be mitigated / accepted.

3.5 Physical and System Access Control

3.5.1 Access control systems are to be implemented to restrict the entry of personnel to areas where critical assets are located. For e.g. propulsion control systems, computer systems for ship shore communication, bridge navigation systems, etc.

3.5.2 The selected access control method is to meet the level of security required at that location, as considered in risk assessment methods.

3.5.3 The access control may be implemented area wise e.g. where only authorized personnel are allowed to enter the area. This could be implemented through a smart card or bio metric system which allows only authorized personnel to enter into a work area.

3.5.4 The organization is to define procedures and implement system access controls. The access control can be network based where only authorized personnel are given rights to enter or can be system based, where the system allows only a particular user to log in. A combination of both the systems is recommended in line with the risk analysis.

3.5.5 The selected control is to be suitable for the type of system i.e. Information Technology (IT) / Operation Technology (OT). The privileged rights for system access are to be restricted and logs of access control are to be maintained.

3.6 Network Security

3.6.1 A network plan clearly identifying all the network components for each on board IT and OT network is to be submitted.

3.6.2 The IT and OT networks are to be protected against unauthorized access from both internal and external sources through implementation of suitable controls. Physical layout of network components is to be considered in implementation of suitable physical, access control as indicated at Cl 3.5 of this section. Network access is to be controlled as per policy.

3.6.3 The ship network is not to be directly connected to internet. Perimeter security is to be provided through suitably configured fire walls. The fire wall configurations are to be in accordance with organization risk management policy

3.7 System security controls

3.7.1 The organization is to implement suitable control measures to ensure its servers, control system servers/controllers and end user systems, against unauthorized access.

3.7.2 All the systems are to be configured in accordance to a baseline configuration. Procedures are to be formulated for software updates and anti-malware installation.

3.7.3 Procedures are to be defined and implemented for system maintenance.

3.8 Detection controls

3.8.1 The procedures and controls for detecting a Cyber incident are to be defined and implemented. The detected events are to be analyzed.

3.8.2 The selected control is to be suitable for the type of system i.e. Information Technology (IT) / Operation Technology (OT).

3.8.3 Ship and shore personnel responsible for implementation of onboard detection control for identified systems are to be identified and their roles and responsibilities are to be defined.

3.8.4 Controls to detect any cyber security events including generation of logs as appropriate are to be implemented.

3.8.5 Cyber security event log management is to be defined.

3.9 Response and Recovery Procedures

3.9.1 A cyber incident response and backup procedure document is to be prepared.

3.9.2 The document is to include details of persons responsible response and recovery activity including their roles and responsibilities.

3.9.3 Storage location of software and hardware required for backup and the authorization required for execution are to be designed.

3.9.4 Communication reporting during response and recovery process are to be defined. The roles and responsibility of the persons executing the response and recovery process are to be defined.

3.9.5 Unresolved issues are to be escalated and polices for the same are to be formulated.

3.10 Training, Awareness and Information sharing

3.10.1 Senior management on board, are to be aware of cyber safety issues and sufficient training is to be imparted to all personnel involved with Cyber-Safety.

3.10.2 The cyber safety awareness may be increased using following methods but not limited to:

- Email communications
- Newsletters
- Videos and DVDs
- Websites and webcasts.

3.10.3 Cyber information is to be shared in an informal way, except in critical / emergency condition.

3.10.4 Cyber safety training needs relevant to the job are to be identified. Training on changes to regulatory requirements are to be imparted for identified personnel.

3.11 Cyber Safety Process Review

3.11.1 Review of the risk assessment and mitigation controls is to be carried out upon any addition of new asset or change in model /make of existing asset.

3.11.2 The revised policies and procedures are to be approved.

3.12 Guidance on the application of requirements to IT systems and control systems corresponding to notation CYS-I, is provided in Annex-I.

Annex I
Guidance for Application of Requirements to IT Systems and Control systems
Notation CyS-I

Governance, Policies & Procedures	**General**
	A cyber safety policy is to be established and communicated to all concerned.
	A business continuity plan in the event of cyber-attack on critical systems is to be approved and documented.
	Operational objectives and activities are to be established, prioritized and communicated to all concerned.
	Governance process is to address cyber security risks at high level.
	Clear definition of roles and responsibilities with regard to cyber safety is to be formulated.
	Legal and regulatory obligations/ requirements with respect to Cyber safety are to be identified.
	A suitable risk assessment approach is to be identified.
	The senior management and employees working on critical cyber systems are to have general awareness on cyber safety.
	Ship cyber safety officer is to be designated who would be responsible for implementation of cyber risk management.
	Procedure for monitoring of regulatory requirements and addressing them is to be formulated.
	Organization Internet and Email policies are to be defined and implemented
	IT
	Defined and approved Information security policies by the management, are to be documented and the same are to be communicated to relevant personnel.
	Responsibilities of information security are to be clearly defined and allocated.
	Where required, a person on board is to be identified to assist ship cyber security officer on information system.
	The selected risk assessment and analysis approach and methodology is to identify and prioritize risks based upon security threats, vulnerabilities and consequences related to their information systems.

	OT
	A high-level system risk assessment is to be performed to understand the safety, operational, environmental effects in the event that, availability, integrity or confidentiality of the ship control system is compromised.
	The personnel responsible for various ship control systems are to be clearly identified and their responsibilities are to be defined.
	The selected risk assessment and analysis approach and methodology is to identify and prioritize risks based upon security threats, vulnerabilities and consequences related to their systems
	The results of physical, HSE and cyber security risk assessments are to be integrated to understand the assets' overall risk.
	All personnel that perform risk management, control system engineering, system administration/ maintenance and other tasks related to control system management are to be trained on the security objectives and operations for these tasks.
	Cyber security policies and procedures that deal with Control System risks are to be consistent with or extensions of policies created by other risk management systems.
	A contingency plan for the critical control systems is to be developed. The plan is to identify control systems required for essential operations of the vessel and evolve contingencies.
	The contingency plan is to identify restoration objectives and priorities for restoration.
	Where required, a person is to be identified to assist the ship cyber safety officer on ship's control system.
Asset Management	**General**
	Ownership of all IT and OT assets is to be identified.
	The inventory is to be updated after any asset change.
	Ship communication and data flows including external communications are to be mapped.
	Resources (for e.g. hardware, devices, data, and software) are to be prioritized based on their classification, criticality, and business value.
	Critical areas having sensitive information and appropriate access control measures are to be identified.
	Systems, loss of which can have impact on critical nature of business undertaken by the ship are to be identified.
	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.
	IT
	All IT Physical systems required for vessel intended operations are to be identified and documented.
	Software platforms installed on board for various applications are to be inventoried.
	Information and information processing facilities assets are to be inventoried.

	Communication and data flow in IT systems are to be identified towards formulation of policies, procedures and controls to protect the data and communication through all types of communication mediums.
	Information is to be classified on the criterion of value, criticality and sensitivity, if it can be compromised due to unauthorized disclosure or modification.
	Vulnerabilities in information systems required for intended operations of the vessel are to be identified.
	OT
	All control systems required for vessel propulsion, safety and navigation systems including systems to effectively carry out the intended operation of the vessel are to be inventoried.
	The organization is to identify the various control systems, gather data about the nature of the security risk, controls systems and group the devices into logical systems. (Propulsion, navigation etc.)
	Control systems software including their version numbers used for vessel propulsion, safety and navigation systems including systems to effectively carry out the intended operation of the vessel are to be inventoried.
	The control systems are to be prioritized based on their criticality to perform vessel functions. A priority rating may be assigned towards mitigation of risks.
	A detailed vulnerability assessment of all individual cyber controlled control systems is to be carried out.
	The organization approves, controls, and monitors information system maintenance tools.
Risk Assessment	**General**
	The organization is to established risk tolerance and acceptance criterion.
	Identification and documentation of consequences of each threat on vulnerable system is to be carried out.
	Approved and documented risk methodology is to be in place.
	Identification of risk priorities based on severity of impact and risk classification is to be carried out.
	Identified risks which can be mitigated / accepted are to be documented.
	Threats, both internal and external, are to be identified and documented.
	Potential business impacts and likelihoods are to be identified and documented.
	Asset vulnerabilities are to be identified and documented.
	Threats, vulnerabilities, likelihoods, and impacts are to be considered during to determination of risk.
	Risk responses are to be identified and prioritized.

	IT
	The organization is to carry out risk assessment of the information system including stored and transmitted information.
	The results of risk assessment are to be documented in risk assessment report.
	The organization is to develop procedures to manage risk to ship operations and assets including individuals who are associated with use and operation of information systems.
	The organization is to consistently implement the risk management strategy.
	OT
	Methods for prioritizing vulnerabilities are to be identified in risk assessment identified in the detailed vulnerability assessment.
	Control system cyber risks that ship faces are to be identified and the likelihood and severity of these risks are to be assessed.
	A detailed risk assessment is to be carried out.
	Risk assessment is to be conducted through all stages of the technology lifecycle.
	The risk assessment is to include the criterion to Reduce risk and maintain risk at an acceptable level.
	Risk tolerance level is to be defined.
	The organization is to determine and document its risk tolerance as a basis for creation of policy and risk management activities.
Physical & System access control	**General**
	Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides.
	Issues authorization credentials for facility access.
	Reviews the access list detailing authorized facility access by individuals.
	Removes individuals from the facility access list when access is no longer required.
	Secure areas are to be protected by appropriate entry controls.
	Removal of Equipment, information or software is to be through prior authorization.
	Requirements for mitigating the risks associated with supplier's access to the ships IT/OT assets are to be agreed with the supplier and documented.
	Security requirements when provided with such access are to be identified and documented.
	Safety levels required for systems/ equipment based on risk assessment are to be identified and implemented.

	The administrative controls for system log are to be implemented.
	Measures to ensure Endpoint Security are to be implemented.
	Removable media is to be protected and its use restricted according to policy.
	Policy to limit the use of external devices e.g. USB devices is to be formulated and implemented.
	Email policy measures are to be implemented.
	The control system is to provide the capability to uniquely identify and authenticate all human users.
	Access accounts are to be role based to manage access to appropriate information or systems for that user's role.
	The allocation of privileged access rights is to be restricted and controlled.
	Identities and credentials are managed for authorized devices and users
	IT
	Areas containing sensitive or critical information and information processing facilities are to be protected through clear definition of security parameters.
	Secure areas are to are to be protected through implementation of appropriate entry controls. to ensure access to only authorized personnel. The secure areas to include delivery and loading areas where the possibility of unauthorized entry of personnel is possible.
	A formal user registration and de-registration process is to are to be implemented to enable assignment of access rights. Create, enable, modify, disables, and remove information system accounts in accordance with defined procedures or conditions.
	Opportunities for unauthorized or unintentional modification are to be reduced through segregation of conflicting duties and responsibilities.
	OT
	Barriers to unauthorized access are to be provided through physical security barriers.
	Procedures for monitoring and alarm are to be provided when physical or environmental security is compromised.
	Authorization security policy is to be defined for granting access privileges.
	Any remote login to the control system is to be controlled and is to be authorized by SCSO.
	Access accounts are to be role based for that user's role. When defining roles safety implications are to be considered.

Network Security	**General**
	All networks in the ship are to be inventoried.
	The organization is to have a policy to maintain network integrity.
	Measures to ensure Perimeter security are to be implemented.
	IT
	All networks serving Information systems are to be inventoried.
	Networks are to be managed and controlled to protect the networks and ensure security of the information.
	OT
	All networks serving ship's control system either in standalone mode (sensor to server network) and or interconnected systems are to be inventoried.
	Access to the control system via un-trusted networks is to be monitored and controlled.
System security controls	**General**
	Anti Malware solutions are to be implanted identified IT and OT systems
	Procedures for software updating and testing of updates are to be formulated and implemented
	A maintenance procedure is to be formulated for equipment required for vessel operations
	Maintenance and break down logs are to be maintained as per defined log maintenance period.
	IT
	Secure areas are to be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
	Prior authorization is to be obtained for moving the equipment, information or software off-site
	Identified Controls to mitigate the risk due access to the ships assets from remote location (outside the ship) are to be implemented.
	OT
	Using clearly defined criteria, proposed changes to Control system are to be reviewed for their potential impact to HSE risks and cyber security risks.
	The control system is to have the capability to be configured according to recommended network and security configurations.
	All assets are to be properly maintained to ensure proper operation.

	The organization is to approve, control, and monitor information system and operational system maintenance tools.
	Detection and prevention controls to protect against malware at server and end user level are to be in place.
Detection Controls	**General**
	Barriers to prevent unauthorized access into critical systems are to be in place.
	The organization is to formulate a policy on removable media.
	Intrusion preventions systems (fire walls etc.) are to be in place.
	Procedures for accessing systems are to be instituted.
	Controls implemented for the systems (IT and OT) are to be suitable.
	A baseline configuration of information technology/control systems is to be created and maintained
	IT
	Procedures are to be developed and implemented for installation of software on operational systems.
	The Organization is to establish and implement the Rules for installation of software by users.
	Critical applications required for business are to be reviewed and tested, whenever there is a change in operating platform, to ensure there is no adverse impact on organizational operations or security.
	Software modifications are to be limited and all changes are to be controlled.
	The organization is to maintain a current baseline configuration of the information system.
	OT
	Proposed changes to control system are to be reviewed for their potential impact to HSE risks and cyber security risks The criterion is to be defined and documented.
	The control system is to provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier.
	The control system is to provide an interface to the currently deployed network and security configuration settings.
	A change management system for the Control system is to be developed and implemented. The change management process is to follow separation of duty principles to avoid conflicts of interest.
Response and Recovery Procedures	**General**
	Methods are to be established and documented for responding to an incident.
	Persons responsible for incident response and back-up are to be clearly identified and their roles defined.
	Each incident is to be recorded and reviewed periodically for lessons learnt.
	Location of software and hardware required for backups are to be documented and inventoried.

	Locations of back-up storage, authorization for backup retrieval are to be defined and documented.
	A back-up policy in the event of cyber system being compromised is to be documented along with procedures for implementation. The document is also to indicate the roles and responsibilities of persons involved.
	The external and internal IT and OT security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan are to be addressed.
	Personnel are to know their roles and order of operations when a response is needed.
	Events are to be reported consistent with established criteria.
	Recovery plan is to be executed during or after an event.
	IT
	Responsibilities response and recovery procedures of IT systems are to be defined and allocated.
	Appropriate contacts with relevant authorities are to be maintained.
	Information security events are to be reported as quickly as possible.
	The organization is to develop a contingency plan for the information system and the plan is to be based on ship essential missions and business functions. The plan is to be approved and is to identify and document recovery objectives, restoration priorities, including roles and responsibilities of relevant personnel
	The contingency plan is to identify recovery objectives and order of priority for restoration of the systems/ equipment.
	The contingency plan is to address roles and responsibilities of the personnel involved in execution of contingency plan.
	The contingency plan is to be protected from unauthorized disclosure and modification.
	OT
	The incident response plan is to be communicated to all relevant personnel.
	Procedure to report unusual activity and events which may actually be cyber security incident is to be established.
	Cyber security incidents are to be reported in a timely manner.
	The details of an identified incident are to be documented to record the incident, the response, the lessons learned, and any actions taken to modify the CSMS in light of this incident.
	General

Training, awareness & information sharing	Key senior personnel who would be involved in top level decisions towards cyber safety implementation are to be identified and communicated.
	Cyber safety training needs relevant to the job are to be identified.
	Mechanism to capture changes in cyber regulatory policies is to be in place.
	Cyber information is to be shared in an informal way, except in critical /emergency condition.
	All users are to be informed and trained.
	Privileged users are to understand roles & responsibilities.
	Senior executives are to understand roles & responsibilities
	IT
	All personnel using information systems are to be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities.
	Responsibilities of information security training, awareness and information sharing are to be clearly defined and allocated.
	OT
	All personnel that perform risk management, control systems engineering, system, administration/maintenance and other tasks that impact the control system management system are to be trained on the security objectives and industrial operations for these tasks.
Cyber Safety Process Review	**General**
	Risk assessment and mitigation controls are to be reviewed upon change on any OT or IT asset make /model number, addition of any new assets.
	The revised policies, procedures and controls are to be approved and documented.

Section 4

Advanced Cyber Safety

4.1 General

4.1.1 The requirements to be complied with, for assignment of Advanced Cyber Safety (**CyS-II**) notation are indicated in this Section. These are to be complied with, in addition to the requirements for assignment of **CyS-I** notation.

4.2 Governance, Policies and Procedures

4.2.1 The policies and procedures are to be reviewed periodically and the revised approved policies are to be communicated to all concerned. The periodicity of review is to be defined.

4.2.2 Procedures are to be established and reviewed with respect to the addition, removal and disposal of all assets.

4.2.3 The implemented controls are to be verified towards compliance to requirements indicated in this section. The results of verification are to be considered during review of policies and procedures.

4.2.4 The security of process control systems can be at risk by third parties e.g. vendors, service suppliers, maintenance supports teams etc. which interact with ship's cyber systems. All the third party vendors, service providers who interact with the ship cyber systems are to be identified

4.2.5 The organization is to enter into an agreement with third party insisting on implementation of basic cyber safety control such as fire walls, antivirus etc. at their end is to be formulated

4.2.6 Where software updates are carried out by third party service providers, a software update process is to be defined.

4.2.7 Specific clauses in contract with third party to manage cyber risk are to be included. Typical clauses are to include non-disclosure agreement, immediate communication of any risk detected by the third party which can affect the ship.

4.3 Asset Management

4.3.1 The asset registry is to include all the ship IT, OT assets and associated networks.

4.3.2 The asset registry is to be reviewed and updated with every

- change in risk profile
- change of flag;
- change of class;
- changes in its IT or OT systems
- Evolving technology

4.3.3 The Organization is to formulate a procedure for patch management. Patch management tasks include maintaining current knowledge of available patches, identify patches appropriate for particular systems and ensure installation of patches in accordance with manufacturer recommendations. The updated software is to be tested and the asset registry is to be updated.

4.3.4 All asset changes are to be managed and asset replacements are to be verified with base line configurations.

4.3.5 Firmware is to be updated as per manufacturer recommendations and updated asset is to be tested. When the asset forms a part of an integrated system, then the complete integrated system is to be tested

4.4 Risk Assessment

4.4.1 Internal threat information, detected and analyzed by the detection process, are to be considered in the risk assessment.

4.4.2 A vulnerability scan is to be performed on IT systems. For carrying out vulnerability testing of OT systems, manufacturer's consent is to be obtained and the testing is advised to be carried out during berthing. The results of above tests and information received from external sources on known vulnerability are to be considered during risk assessment.

4.4.3 Documented and approved procedures and processes to carry out risk assessment and the controls implemented towards risk mitigation of ship's IT and OT systems are to be reviewed and updated as required

4.4.4 Risks indicators and threats are to be regularly reviewed and updated where found necessary

4.4.5 Information about technical vulnerabilities of information systems being used are to be obtained in a timely fashion, the ship's exposure to such vulnerabilities is to be evaluated and appropriate measures taken to address the associated risk

4.4.6 Risk management process which includes periodical review of threats, vulnerabilities, identification of new threats is to be formulated, implemented and maintained.

4.4.7 Data integrity risks and Consequences of accepted and residual risks are to be reviewed periodically

4.4.8 Risk management processes are to be established, managed and agreed to by stakeholders, as appropriate.

4.4.9 External penetration testing is required to be conducted to identify weaknesses in the ship's network which could allow an attacker to access the systems. Special care is to be taken when performing penetration tests on live (in-production) systems. Penetration testing is to be considered especially when employing new technology or processes as well as when the risk picture has changed.

4.4.10 Following requirements are to be complied with as applicable:

- Goals for penetration testing are to be clearly defined and the same is to be communicated to the test team
- The network architecture is to be evaluated for an appropriate defense-in-depth security strategy
- A strategy for using firewalls is to be developed and functional demilitarized zone DMZs are to be established
- Information which can be shared with test team as per the desired mode of testing i.e. black box, grey box or white box testing, is to be clearly defined.

4.5 Physical and System Access control

4.5.1 Access control measures are to be reviewed periodically. Detected access breach incidents are to be considered in review.

4.5.2 Suitable measures are to be identified and implemented to address the identified issues.

4.5.3 Base line authentication procedures for remote users are to be implemented.

4.5.4 For system access control advanced authentication controls are to be implemented. Implementation of physical and system access controls can be function specific or zone specific.

4.5.5 The physical access for identified critical areas are to be monitored for cyber-security events.

4.5.6 The procedures and controls are to be reviewed periodically. Information on new threats, breaches are to be analyzed and existing process is to be reviewed / updated as required.

4.6 Network Security

4.6.1 In addition to perimeter security and creation of Demilitarised Zone (DMZs), the network security is to be augmented by provision of VPNs and VLANs.

4.6.2 Formal transfer policies, procedures and controls are to be in place to protect the transfer of information through the use of all types of communication facilities.

4.6.3 The control system is to provide the capability to deny external network traffic by default and allow network traffic by exception.

4.6.4 Communication and control networks are to be protected.

4.6.5 The organization is to implement a suitable security monitoring method and a procedure to determine the impact of events is to be established. Following methods may be used as applicable:

Intrusion Detection Systems (IDS) based on signature matching algorithms. The systems can be network based or specific to one equipment.

- Network based intrusion detection is to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting.
- Host based intrusion detection system (HIDS), is to identify unauthorized, illicit and anomalous behavior on a specific device. The role of a host IDS is passive, only gathering, identifying, logging, and alerting.
- Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection systems may act as prevention systems. Examples of Physical intrusion detections may be

    - Security Guards
    - Security Cameras
    - Access Control Systems (Card, Biometric)
    - Motion Sensors

4.6.6 Intrusion prevention has the same process of gathering and identifying data and behavior, with the added ability to block (prevent) the activity. This can be implemented with Network, Host, or Physical intrusion detection systems.

4.6.7 Procedures are to be in place to assess the requirements of detection process when any new system is added/ replaced

4.6.8 The organization is to formulate policy to maintain network integrity and is to establish incident thresholds

4.6.9 The controls used for the detection process are to be regularly updated and tested in line with latest technology

Network Segmentation

4.6.10 Network segmentation involves apportioning of networks into small networks with clearly defined rules on which systems/ users can communicate from/ to a network. This may be achieved by:

- Division of large networks into separate network domains (segments);
- Consideration of physical and logical segregation;
- Definition of domain perimeters;
- Definition of traffic rules between domains;
- Usage of authentication, encryption, and user-level network access control technologies.

Mobile Device Security

4.6.11 When the ship control and information systems can be accessed from a mobile control are to be implemented for a secured connectivity.

4.6.12 Usage restrictions, authorizations and monitoring of mobile devices are to be formulated and implemented.

4.6.13 All unauthorized connections of mobile devices to ship network systems are to be monitored.

Wireless Device Security

4.6.14 The control system is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

4.6.15 Procedures are to be defined and necessary controls are to be implemented to comply with following requirements for wireless device security as applicable:

- Usage restrictions and implementation guidance for wireless access are to be established
- Unauthorized wireless access to the information system is to be monitored
- Wireless access to the information system prior to connection is to be authorized

4.7 System Security Controls

Data security

4.7.1 The organization is to implement suitable controls to ensure data security.

4.7.2 Each time data is replicated or transferred, it is to remain intact and unaltered between updates.

4.7.3 Error checking methods and validation procedures are to ensure the integrity of data that is transferred or reproduced without the intention of alteration.

4.7.4 Data integrity may be compromised in a number of ways:

- Human error, whether malicious or unintentional
- Transfer errors, including unintended alterations or data compromise during transfer from one device to another
- Bugs, viruses/ malware, hacking and other cyber threats
- Compromised hardware, such as a device or disk crash
- Physical compromise to devices.

4.7.5 Data security is one of several measures which can be employed to maintain data integrity, as unauthorized access to sensitive data can lead to corruption or modification of records and data loss.

4.7.6 Policies and procedures for management of information data in accordance with its defined risk strategy are to be developed. The procedures to store confidential data and its protection are to be formulated

4.7.8 Procedures to protect data in transit or when it is residing in host servers are to be formulated.

Information Protection process

4.7.9 The processes and procedures for information protection are to be established.

4.7.10 Security policies clearly identifying the purpose, scope, roles, responsibilities and coordination are to be established.

Cryptography

4.7.11 The system is to have the capability to protect the confidentiality of information at rest, during remote access sessions and during traversing of an un-trusted network is to be provided. Encryption is a common mechanism for ensuring information confidentiality.

4.7.12 A base line configuration is to be formulated and change management process is to be implemented.

4.7.13 Data backup management and data destruction policies and procedures are to be defined and implemented.

4.7.14 Plans for incident handling are to be formulated

4.7.15 The policy towards continual improvement of protection process is to be formulated and implemented.

4.8 Detection Controls

Anomalies and events

4.8.1 Advanced threat Detection techniques ex. Anomaly Detection (AD) and Network Behavior Anomaly Detection (NBAD) are to be implemented for threat detection.

4.8.2 Network Behavior Anomaly Detection (NBAD) approach may be used to network security threat detection. NBAD is the continuous monitoring of a network for unusual events or trends.

4.8.3 An NBAD program is to track critical network characteristics in real time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Large-scale examples of such characteristics may include traffic volume, high bandwidth use etc.

4.8.4 NBAD solutions may also be used to monitor the behavior of individual network subscribers. NBAD is to be used in addition to conventional firewalls and applications for the detection of malware.

4.8.5 A cyber safety center is to be setup in a suitable location from where all the cyber safety issues, monitoring of various cyber safety parameters, access control, business continuity, disaster management can be supervised/ controlled by suitable designated person.

4.8.6 The cyber safety centre may be supported by shore based security operations centre. In such cases the logs generated by the ship are to be forwarded to the SOC for analysis and for further instructions/advice to ship. The SOC may act as centralized nodal point for fleet of ships to address cyber issues.

4.8.7 Procedures and controls are to be defined and implemented to detect and analyze anomalous activities in timely manner.

4.8.8 Procedure to analyze the behavior of individual network traffic to form a base line is to be defined.

4.8.9 detected anomalies are to be analyzed to evaluate potential impact on ship critical systems. Procedures for communication and immediate action when an anomaly is detected are to be formulated.

4.8.10 A periodical review of the detection process is to be undertaken.

4.8.11 Advanced technological tools in the field of computer security, security information and event management (**SIEM**) software products are to be implemented. The SIEM combines the services of security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by network hardware and applications.

4.8.12 Monitoring system and network for changes, anomalous behaviors, or for attack signatures are essential to the Defense-in-Depth concept of protecting critical assets.

4.8.13 Security information management (SIM) and security event management (SEM) are to be implemented. They provide real-time analysis of security alerts generated by network hardware and applications. The network is to be monitored on a continuous basis.

4.8.14 Procedure for monitoring external service providers' activity and monitoring of unauthorized personnel connections is to be developed and implemented.

- Activity of external service provider is to be monitored to detect potential cyber security events;

- Monitoring for unauthorized personnel, connections, devices, and software is to be performed;

4.9 Response and Recovery procedures

Response Procedures

4.9.1 Processes and procedures to identify and respond to threats are to be defined and documented.

4.9.2 The methodology of handling IT/ OT cyber incidents is to be defined.

4.9.3 The organization is to have Cyber Safety Response Team (CSRT) to deal with all types of cyber threats.

4.9.4 The rules, roles and responsibilities of the response team are to be clearly defined.

4.9.5 The organization is to have procedures and methods to regularly monitor and update its response plans. Process for early warning system and means to communicate are to be clearly defined.

Recovery Procedures

4.9.6 Effective recovery planning is a critical component of ship/s preparedness for cyber event. Recovery planning is to enable participants to understand system dependencies, critical personnel identities such as crisis management and incident management roles, arrangements for alternate communication channels, alternate services, alternate facilities etc.

4.9.7 The planning and documentation for recovering from a cyber-security event is to be in place before the cyber event occurs.

4.9.8 The backup and recovery procedures are to be periodically reviewed. The review periodicity is to be defined.

4.9.9. Procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information are to be formulated.

Communication

4.9.10 The type of communication required is to be defined by the type of incident and its potential impact.

4.9.11 Communication control (both internal and external) is to ensure that right information is communicated at the right moment by the right senders to the right receivers. Controls are to address communication openness and protection.

4.9.12 A list of potential stakeholders is to be prepared and procedures are to be defined to ensure that the right contact information is available for effective communication. Information required to be communicated to every person is to be clearly defined.

4.9.13 Ways of communications for internal stake holders are to be clearly defined. The ship has to identify alternative secure communication channels and the process to be followed after a cyber-incident.

4.9.14 When an actual cyber safety incident occurs, the cyber safety incident response team is to immediately draw up a concrete communication plan for the specific incident. Effective procedures towards the same are to be documented.

4.9.15 All the internal stake holders who need to be communicated in an emergency including the communication methodology. are to be identified

4.9.16 Authorization and communication media are to be defined.

4.9.17 Coordination with stakeholders is to be carried out in accordance with established response plans.

4.9.18 A disaster recovery plan is to be formulated, approved and tested periodically. The personnel involved identified in disaster recovery plan are to be communicated about their roles and responsibilities in the event of disaster.

4.9.19 The organization is to establish a process to analyze the incidents through an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

4.10 Training, awareness and information sharing

4.10.1 The security of process control systems is to be improved by increasing awareness, improving skills and techniques

4.10.2 Cyber safety awareness programs are to provide insights into threats and risks to various control systems including the technical and procedural solutions that can be deployed to prevent cyber safety attacks from succeeding.

4.10.3 The training is to cover a wide technical area, ranging from IT skills to process control skills. Organizations are to develop customized training frameworks to ensure that personnel have the appropriate skills and knowledge to perform their jobs securely.

4.10.4 A training framework is to be developed that covers training for the key personnel, detailing the level of understanding of an organization's vulnerabilities, the information and resources that can be accessed to share good practices and approved mitigation measures.

4.10.5 Process to update its senior management on impact of cyber risks on legal and business aspects are to be defined.

4.10.6 Process to identify the training needs by the line manager (reporting officer on ship) is to be established. Training topics are to address various aspects for successful implementation of onboard cyber risk management. Ex. operations, software updates, threats, vulnerabilities, maintenance, access controls, security controls etc.

4.10.7 Procedures are to be established and implemented for conducting an effective training.

4.10.8 Effective communication of updated information on cyber safety is made to its employees through various communication media. For e.g. emails, seminars, workshops, etc.

4.10.9 All the personnel involved in cyber safety including the third party stake holders are to be trained to perform the designated duties related to ship cyber systems.

4.10.10 The training is to include evolving technologies, new threat perception from industry and risk approach methods.

4.10.11 The personnel involved in analysis of event logs and operation of SIEM are to be trained for use and operation of SIEM tools.

Evolving Technologies and Information Sharing

4.10.12 Cyber Safety is a dynamic subject and procedures are to be in place to keep the ship staff technically updated on new technologies, new threats and industry feedback. In the larger context, procedures to share its cyber related incidents with others and at same time learn from industry are to be formulated and implemented.

4.10.13 A holistic view of the total environment which includes external factors needs to be taken into account in this level of implementation. Examples of external context may include:

- Changes which can effect ship operations;
- Evolving technological changes which effect vessel efficiency.

4.10.14 The organization is to have a policy on receiving and sharing cyber threat information. The criticality of ship operations are to be established and process is to be established to assimilate information from similar shipping companies and industries where such technologies (cyber systems) are used.

4.11 Cyber Safety Process Review

4.11.1 The cyber safety technical controls and procedures are to be reviewed periodically. The periodicity of review is to be defined.

4.11.2 The threat information results received from the analysis of detected threats, is to be considered in the review process.

4.11.3 Threat information from similar industries received from various forums is to be considered in risk analysis.

4.11.4 The organization has to assess its current state of implementation of cyber risk management process and is to continually work on them for further improvement.

4.11.5 A process to undertake continual improvement of their cyber safety systems is to be developed based on threat perception and technological changes.

4.11.6 A current profile of ships' cyber risk practices is to be prepared and its progress is to be monitored for implementation of cyber safety practices

4.11.7 The existing cyber safety policies are to be reviewed periodically and changes are to be evaluated and implemented where considered necessary through changes in controls.

4.11.8 The organization has to regularly carry out its cyber safety audits and allocate necessary budget.

4.11.9 The organization continuously is to review and improve the existing process, procedures, effectiveness, information /data security management systems.

4.11.10 The organization is to formulate criterion for software procurement / design and is to periodically review policies on mobile , wireless connectivity, remote logins.

4.11.12 Asset and cyber security event management process are to be periodically reviewed.

4.11.13 Access control management event Log management process and procedures are to be periodically reviewed.

4.12 Guidance on the application of requirements to IT systems and control systems corresponding to notation CYS-II, is provided in Annex-II.

Annex II
Guidance for Application of Requirements to IT systems and Control systems
Notation CYS-II

Governance, Policies & Procedures	**General**
	All the third party vendors, service providers who interact with the ship cyber systems are to be identified.
	An agreement with third party insisting on implementation of basic cyber safety control such as fire walls, antivirus etc. at their end is to be formulated; Responsibilities of third party are to be clearly defined.
	Responsibilities are to be clearly defined for cyber security and related physical security activities.
	Specific clauses in contract with third party to manage cyber risk are to be included. Typical clauses are to include non-disclosure agreement, immediate communication on any detected risk by the third party which can affect the ship.
	Position in critical infrastructure and its industry sector is to be identified.
	Dependencies on critical infrastructure and critical services are to be established.
	Resilience requirements to support critical infrastructure are to be identified and communicated.
	Criticality analysis is to be used to identify critical information system components and functions.
	Knowledge of its role in the larger ecosystem, but has formalized its capabilities to interact and share information externally.
	IT
	Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) towards information systems are to be established.
	Patch updating process with third party software providers is to be formulated.
	Policy is to be formulated and implemented to ensure that all employees and contractors apply established polices of information security
	OT
	Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) towards ship control systems are to be established.
	All personnel (including employees, contract employees, and third party contractors) are to be trained initially and periodically thereafter in the correct security procedures and the correct use of Control systems.
	General
	The asset registry is to include all the ship IT, OT assets and associated networks.

Asset Management	The assets register is to be updated for any of following conditions • change in risk profile • change of flag; • change of class; • changes in its IT or OT systems • Evolving technology
	Patch management tasks are to include maintaining current knowledge of available patches, identify patches appropriate for particular systems and ensure installation of patches in accordance with manufacturer recommendations.
	A base line configuration is to be established and replaced assets are to be verified with base line configurations;
	The asset inventory is to be current
	IT
	The updated system /application/database software is to be tested and the asset registry is to be updated.
	OT
	Firmware is to be updated as per manufacturer recommendations and updated asset is to be tested. When the asset forms a part of an integrated system, then the complete integrated system is to be tested
Risk Assessment	**General**
	Risks indicators and threats are to be regularly reviewed and updated where found necessary.
	Threat and vulnerability information is received from information sharing forums and sources.
	Any new identified threats are to be documented and risk analysis is to be carried out.
	Each cyber safety related incident is to be recorded and reviewed periodically for lessons learnt.
	Methods are to be formulated and implemented to assess and address data integrity risks.
	Consequences of accepted and residual risks are to be reviewed periodically.
	Vulnerability scans are to be performed and results are to be used in risk assessment.

	Determination of risk tolerance is to be decided by its role in critical infrastructure and sector specific risk analysis.
	Information about technical vulnerabilities of information systems being used are to be obtained in a timely fashion, the ship's exposure to such vulnerabilities is to be evaluated and appropriate measures taken to address the associated risk.
	Periodic reviews of risk management process for IT and OT systems are to be carried out. The document is to define the periodicity of review.
	Risk management processes are to be established and managed.
	Goals for penetration testing are to be clearly defined and the same is to be communicated to the test team.
	The network architecture is to be evaluated for an appropriate defense-in-depth security strategy.
	A strategy for using firewalls is to be developed and functional demilitarized zone DMZs are to be established.
	Information which can be shared with test team as per the desired mode of testing i.e. black box, grey box or white box testing, is to be clearly defined
	IT
	Knowledge gained from analyzing and resolving information security incidents is to be used to reduce the likelihood or impact of future incidents.
	Penetration testing is to be carried out on identified information systems. The frequency testing is to be identified and documented.
	Risk assessment is to be conducted to assess the likelihood and magnitude of harm of the information system and the information it processes, stores, or transmits.
	Risk assessment results are to be documented in risk assessment report.
	Risk assessment results are to be reviewed periodically as per defined frequency.
	OT
	Identify the set of Control system cyber risks that a ship faces and assess the likelihood and severity of these risks.
	A detailed risk assessment incorporating the identified vulnerabilities is to be conducted.

	Risk assessment is to be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement.
	Penetration testing for control systems networks is to be carried out as per control system manufacturer recommendations. The testing is recommended to be carried out when the vessel is idling at harbour.
Physical & System access control	**General**
	Areas where critical assets are located are to be identified and controls are to be in place to monitor such locations.
	IT
	Computers installed with critical application software and identified as vulnerable are to be provided dual authentication controls
	OT
	Dual authentication controls are to be implemented for critical high risk control systems
Network Security	**General**
	In addition to perimeter security and creation of Demilitarized Zone (DMZs), the network security is to be augmented by provision of VPNs and VLANs.
	Formal transfer policies, procedures and controls are to be in place to protect the transfer of information through the use of all types of communication facilities.
	The control system is to provide the capability to deny network traffic by default and allow network traffic by exception.
	Communication and control networks are to be protected.
	Usage restrictions and implementation guidance for ship controlled portable and mobile devices are to be formulated.
	Connection of mobile devices is to be authorized meeting defined usage restrictions and implementation guidance.
	Monitoring for unauthorized connections of mobile devices to ship information systems is to be undertaken.
	Usage restrictions and implementation guidance for wireless access are to be established.
	Unauthorized wireless access to the information system is to be monitored.
	Wireless access to the information system prior to connection is to be authorized.
	Division of large networks into separate network domains (segments).
	Consideration of physical and logical segregation.
	Domain perimeters are to be defined.
	Traffic rules between domains are to be defined.
	Usage of authentication, encryption, and user-level network access control technologies.
	IT

	Access rights for privileged users to access network devices are to be restricted and controlled.
	Information in systems and applications are to be protected through control of Networks.
	Users are to be provided with access to the information system network and network services that they have been specifically authorized to use.
	Procedures are to be documented and implemented for installation of software on operational systems.
	Acceptable and unacceptable mobile code and mobile code technologies are to be defined.
	Usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies are to be established.
	Authorization, monitoring, and control of the use of mobile code within the information system is to be conducted.
	Usage restrictions, configuration/connection requirements, and implementation guidance for wireless access are to be established..
	Wireless access to the information system prior to allowing such connections is to be authorized.
	Procedures for authentication, encryption, and user-level network access control technologies are to be implemented.
	OT
	Users are to be provided with access to the control system network and network services that they have been specifically authorized to use.
	The control system is to provide the capability to protect the integrity of transmitted information.
	The control system is to have the capability to protect the session integrity and to reject any usage of invalid session IDs.
	Control system devices with common security controls are to be grouped into zones in order to manage security risks and to achieve a desired target security.
	The control system is to have the provision to physically or logically segment OT networks from IT network.
	The system also to have capability to logically segment critical control system networks from other control system networks.
	The control system is to have the capability to identify and authenticate all users (Personnel, software processes or devices) engaged in wireless communication.
System security controls	**General**
	Policies and procedures for management of information data in accordance with its defined risk strategy are to be developed.
	Procedures to store confidential data and protect it from unauthorized access are to be developed.

	Back-up procedures for critical data are to be identified.
	Procedures to protect data in transit and data at rest are to be developed and implemented.
	The control system is to provide the capability to protect integrity of sessions and is to reject any usage of invalid session IDs.
	Procedures are to be implemented to control the installation of software on operational systems;.
	Detection, prevention and recovery controls to protect against malware are to be implemented.
	A baseline configuration for IT systems is to be defined.
	A baseline configuration for OT systems is to be defined.
	Configuration change control process is to be established.
	Systems backup are to be taken at clearly defined back up period. Procedure for testing the backs ups is to be established.
	The physical operating environment for various IT and OT assets are to be established and documented.
	Process and procedure for destruction of data is to be clearly defined.
	A process to continually improve the protection process is to be available.
	Incident response plans are to be established.
	Incident recovery plans are to be established.
	Disaster recovery plans are to be established.
	Procedures and processes for testing response and recovery plans are to be available.
	Practices to include cyber safety issues in human resources practices e.g. personnel screening are to be established.
	Vulnerability management plan is to be established and implemented.

	Access to systems and assets is to be controlled, incorporating the principle of least functionality.
	IT
	Asset handling procedures are to be developed as per information handling scheme and implemented.
	Networks are to be managed and controlled to protect information in systems and applications.
	Communication and data flow in IT systems are to be identified towards formulation of policies, procedures and controls to protect the data and communication through all types of communication mediums.
	Information in electronic messaging is to be protected as appropriate.
	Information is to be protected for its confidentiality, integrity and availability where required backups of critical information are taken as per agreed backup policy.
	Information classification scheme adopted by organization are to be used to develop and implement procedures for handling assets.
	Network and network services are to be access controlled.
	Business and information security aspects are to be considered towards development and implementation of an access control policy for the ship.
	Segregation of information services, users and information systems are to be grouped as per defined policies.
	Changes to, business processes, information processing facilities and systems that affect information security is to be controlled.
	Procedures for installation of software are to be established and implemented.
	Effects on business critical applications whenever the operating platforms are changed are to be reviewed and tested. It is be ensured that there is no adverse impact on operations or security due to above changes.
	Backup policy is to be established and implemented. The backup copies are to be tested at periodically as per defined back up policy.
	Procedures and controls required to ensure and maintain the operations in adverse condition are to be identified and established.
	Equipment is to be located with adequate protection s to reduce the risks from environmental threats and hazards, and unauthorized access.
	Assets are to be handled as per developed procedures for handling assets in accordance with the organization adopted information classification scheme.
	Procedures are to be implemented for the management of removable media.
	Utility programs having capability to override system or application controls are to be restricted and controlled.
	Information flow between systems and sub systems is to be as per approved policies.

	OT
	The control system is to have the capability to protect the confidentiality of information at rest or in transit.
	The control system is to have the capability to remove all information for those decommissioned equipment which had explicit read authorization.
	The control system is to provide the capability to detect, record, report and protect against unauthorized changes to control system software and information at rest.
	The control system is to employ cryptographic methods and is to have the capability to recognize changes to information during communication.
	The control system in general is to deny network traffic by default and allow network traffic by exception.
	Anomalies discovered during operation and or scheduled maintenance are to be reported and the control system is to have the capability to verify the operations of security functions
	A change management system for the Control system is to be developed and implemented.
	The control system is to have the capability to prevent unauthorized and unintended information transfer volatile shared memory.
	Policies and procedures to address both physical and cyber security risks towards protection of assets are to be established.
	Control system is to have the ability to carry out backups of user-level and system-level information without affecting normal plant operations.
	A procedure for backing up and restoring computer systems and protecting backup copies is to be established, used, and verified by appropriate testing.
	The control system is to have the capability to recognize changes to information during communication.
	On all interfaces, the control system is to provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.
Detection Controls	**General**
	Procedures and controls are to be defined and implemented to detect and analyze anomalous activities in timely manner.
	Procedure to analyze the behavior of individual network traffic to form a base line is to be defined.
	Potential impacts of detected anomalies are to be identified.
	All IT and OT systems are to be monitored at regular intervals for unusual activities and breaches.
	Procedures for communication and immediate action when an anomaly is detected are to be formulated.
	Implementation of detection process such as fire walls, intrusion detection and prevention systems to identify threats is to be carried out.

	Periodic evaluation of overall security management system to ensure the security objectives are met and detection processes are continuously improved; is to be carried out.
	Investigation of notifications from detection systems is to be undertaken.
	Detected events are analyzed to understand attack targets and methods
	The detection process is to be regularly updated and tested in line with latest technology.
	Procedures are to be in place to assess the requirements of detection process when any new system is added/ replaced.
	Process for various types of detection methods based on criticality and vulnerability of the systems are to be identified.
	Incident thresholds are to be established.
	Event data are to be aggregated and correlated from multiple sources and sensors.
	Impact of events is to be determined.
	The network is to be monitored to detect potential cyber security events
	Following activities in general are to be carried out at the centre: (a) Network monitoring to detect potential cyber security events (b) Personnel activity monitoring to detect potential cyber security events (c) Monitoring for unauthorized personnel, connections, devices and software vulnerability scans
	IT
	The organization is to establish procedures which would result in a review of existing controls. The procedures are to establish triggers with thresholds to review controls at a minimum: occurrence of security incidents, changes to risk and system including regulatory changes.
	The thresholds are to be based on the defined risk tolerance.
	Management responsibilities and procedures to ensure an appropriate response to information security incidents is to be established.
	Procedures are to be established to obtain information on ship systems technical vulnerabilities. The Ship's exposure to such vulnerabilities is to be evaluated and measures are to be implemented to mitigate any identified risks.
	Event logs capturing user activities, exceptions, faults and information security events are to be maintained and reviewed periodically.
	A continuous monitoring strategy is to be developed and implemented. The monitoring program is to include definition of metrics and monitoring. The frequency of monitoring is to be defined.

	Assessment of existing security control is to be carried out.
	The organization is to have a established monitoring program which includes reporting of the security status to identified personnel
	OT
	The control system is to provide the capability to generate log records relevant to security.
	Individual log records are to include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.
	The system is to have sufficient storage capacity for log management and system configuration.
	The details of an identified incident are to be documented to record the incident, the response, the lessons learned, and any actions taken to modify the control system management system in light of this incident.
Response and Recovery Procedures	**General**
	The organization is to have Cyber Safety Response Team (CSRT) to deal with all types of cyber threats.
	The rules and responsibilities of the CSRT are to be clearly defined.
	The organization is to have procedures and methods to regularly monitor and update its response plans.
	Process for early warning system and means to communicate are to be clearly defined.
	Notifications from detection systems are to be investigated
	Well defined recovery and back up procedures are to be formulated and documented.
	Critical systems and data which need to be recovered in the event of cyber-attack are to be identified.
	Locations of back up storage, authorization for retrieval for backups are to be defined and documented.
	Personnel, teams who are responsible for recovery are to be identified.
	Procedures are to be formulated to train personnel in backup and recovery process.
	Procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information are to be formulated.
	A documented emergency plan is to be available on board.
	All the internal stake holders who need to be communicated with, in an emergency, are to be identified.
	Ways of communications for internal stake holders are to be clearly defined.
	Information required to be communicated to every person is to be clearly defined.
	All the external stake holders who are required to be communicated in emergency are to be identified.

	Mode of communication to external stakeholders is to be defined.
	Extent of information which needs to be communicated is to be defined.
	Any specific authorization required before communicating sensitive information is to be established.
	Communication to media is to be defined i.e. what to communicate and who would communicate.
	Redundant communication paths, in the event of loss of primary communication path are to be identified.
	IT
	Response to Information security incidents are to be as per established procedures.
	Procedures are to be established to use the knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.
	Event logs of user activities, exceptions, faults and information security events are to be regularly reviewed.
	An incident handling capability for security incidents is to be implemented to include containment and recovery.
	Incident handling activities are to be coordinated with contingency planning activities and changes identified upon review of ongoing incidents.
	OT
	An incident response plan is to be implemented. The plan is to identify responsible personnel and actions to be performed.
	An incident is to be identified, then it is to be promptly responded in accordance with the approved procedures.
	Failed and successful cyber security breaches are to be identified
	Appropriate corrective and preventive actions are to be identified and implemented to meet security objectives.
Training, awareness & information sharing	**General**
	Process to update its senior management on impact of cyber risks on legal and business aspects are to be defined.
	A formal process to identify the training by the line manager is to be in place.
	Provision is to be made for subject matter external experts for training.
	Training requirements that address internal threats, lessons learnt and external cyber information are to be defined.

	Specific programs to train its employees on Operation technology and Information technology are to be established.
	Effective communication of updated information on cyber safety is made to its employees through various communication media. For e.g. emails, seminars, workshops, etc.
	Procedures to implement preventive maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; are to be covered as part of training.
	The organization is to have a procedure for receipt of information that enables collaboration and risk-based management decisions in response to events is to be ensured.
	Information is to be actively shared to ensure that accurate, current information is distributed and consumed to improve cyber safety before a cyber-security event occurs.
	IT
	All personnel are to be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities.
	Provision for training the ship staff by the IT system manufacturer is to be implemented. The effectiveness of training is to be ascertained.
	Information security events are to be reported through appropriate management channels Knowledge gained from analyzing and resolving information security incidents are to be shared.
	Access authorizations assigned to the sharing partner are to match the access restrictions for information sharing.
	Processes are to be defined to assist users in making information sharing/collaboration decisions.
	Voluntary information sharing is to occur with external stakeholders to achieve broader cyber security situational awareness.
	OT
	The organization is to provide role-based security training to personnel with assigned security roles and responsibilities.
	Training on control systems is to be carried out Before authorizing access to the system or performing assigned duties or when required by system changes.
	The organization is to have program to train its personnel on recent developments on control and automation systems.
	Provision for training the ship staff by the control system manufacturer is to be implemented. The effectiveness of training is to be ascertained.

	The control system is to provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.
	The organization implements a Control systems threat awareness program that includes a cross-organization information-sharing capability.
	Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
Cyber Safety Process Review	**General**
	A current profile of ships' cyber risk practices is to be prepared and the extent to which it has progressed in implementation of cyber safety practices to meet the five functional requirements specified in cyber safety philosophy: *Identify, Protect, Detect, Respond,* and *Recover*, is to be carried out.
	Policies and procedures with respect to changes in international/ national scenarios are to be reviewed.
	The above information is to be used to re-prioritize resources to strengthen other cyber safety practices.
	Commitment towards cyber safety through repeated successful audits is to be exhibited consistently, so that cyber safety becomes an organizational culture.
	Capital planning is to be catered by way of budget allocation for cyber safety.
	A system to receive threat and vulnerability information from information sharing forums and sources is to be implemented.
	The current profile and the target profile are to be compared to determine gaps.
	The existing process, procedures, effectiveness, information /data security management systems are to be continuously reviewed and improved.
	Procedures are to be established and audited with respect to the addition, removal and disposal of all assets.
	Event detection information is to be communicated to appropriate parties.
	Voluntary information sharing is to occur with external stakeholders to achieve broader cyber security situational awareness.
	IT
	The organization is to formulate procedures for employee personnel data management, in addition to informational data security.
	Data System is to be designed with adequate capacity.
	The organization is to develop a policy addressing remote login by a user and/ or remote connections. Additional controls to automatically terminate remote access may be implemented as per the risk assessment.
	The cyber-attack detection methods for information system are to be periodically tested and continuously improved.

	A system to receive threat and vulnerability information for the information system from information sharing forums and sources and manufacturer is to be implemented.
	OT
	The details of an identified incident are to be documented to record the incident, the response, the lessons learned, and any actions taken to modify the control system management system) due to the incident.
	The organization is to establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk and major changes to the CS. The thresholds are to be based on the ship's risk tolerance.
	A policy addressing remote login for OT systems by a user and/ or remote connections is to be developed. Additional controls to automatically terminate remote access may be implemented as per the asset desired security level.
	The cyber-attack detection methods for control system are to be periodically tested and continuously improved.
	A system to receive threat and vulnerability information for the control system from information sharing forums and sources and manufacturer is to be implemented

References

- IMO guidelines on cyber risk management
- ISO/IEC 27001 standard on Information technology – Security techniques
- ISO/IEC27032-Guidelines for Cyber security
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Security (the NIST Framework).
- Code of Practice - Cyber security for ships by Department of Transport UK
- IEC 62433-2-1 Establishing an Industrial automation and control system security program
- IEC 62443-3-3 Industrial Communication Networks - Network and System Security - Part 3-3: System Security Requirements Security Levels
- ISO 31000 – Risk Management-Principles and Guidelines

End of Guidelines