# Recommendation on incorporating cyber risk into ISM

# No.

00)

(xxx 20xx)

(Rev.1

xxx 20xx)

…

(Rev.x

Xxx 20xx)

Subtitles - \*Arial 11 Bold\*

Main text - \*Arial 11\*

\*Line spacing 1 throughout”

1) “No. xx” should be replaced by relevant Number, i.e. (“No. 10”, “No. 47”, “No. 150”, etc.)

# Foreword

Adopted in 2017, IMO Resolution MSC.428(98) on maritime cyber risk management in safety management systems affirms that “*an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code*”. In other terms, IMO requires shipowners to implement ashore and onboard their vessels an efficient and auditable cyber security risk management.

Section 1.2.2 of the ISM Code stipulates that “safety management objectives of the Company should ./.. “*assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards*”.

Section 10.1 of the ISM Code stipulates that “*the Company should identify equipment and technical systems the sudden operational failure of which may result in hazardous situations. The SMS should provide for specific measures aimed at promoting the reliability of such equipment or systems*.”

Being able to perform a cyber security risk assessment is therefore considered as part of implementing an efficient cyber security risk management, as required by IMO. Far from being a constraint, this should be seen by the shipowner as an opportunity to have a complete view of the OT and IT systems on board his ships, but also, and above all, to know which systems are critical, and how he will be able to implement measures likely to lower the cyber risk to an acceptable and assumed level.

Implementing an efficient cyber security management is paramount, and will be helped by this recommendation. Readers are invited to turn to the following documents which describe in a simple and complete way all the rules and good practices to use in order to effectively manage the field of embedded cyber security:

* MSC-FAL 1/Circ.3 “Guidelines on maritime cyber risk management”
* “The Guidelines on Cyber Security onboard ships” produced and supported by BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)
* BIMCO “Cyber Security Workbook for on board ship use”

These guidelines provide high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this International Maritime Organization.

# Introduction

## Purpose of the recommendation

### Risk analysis is one of the foundations of any risk management. Cyber security is no exception. Therefore the purpose of this document is to propose a method to guide stakeholders on the achievement of a cyber risk assessment for ships in service.

### Using this method is not mandatory, as other methods can be used to perform a risk assessment, such as:

### NIST Guide for Conducting Risk Assessments

### ANSSI EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

### ENISA BS 7799-3 (Information security management systems)

### ISO/IEC 27005:2008 (Information security risk management)

### NIST SP 800-39 (Managing Information Security Risk).

### Version 4 of BIMCO “Guidelines on cyber security onboard ships” contains a method that may be used as well as a basic approach to risk assessment.

### The method presented in this document has the advantages of being relatively simple and adapted to the maritime world. As such, it represents an appropriate complement to IMO Resolution MSC.428(98). This recommendation is not intended to standardize risk assessment methods, but just to provide examples that can be used as reference when relevant parties consider them.

### The proposed risk assessment methodology uses the following principles:

* + - * Threats on critical systems are studied by relying on the consequences, should the threat occur, for confidentiality, integrity, availibility and traceability.
      * Cyber incidents are studied for their impact on the vessel safety and on the continuity of operational activities.
      * Impact and Likelihood determine a Risk Level, which will be referred to for possible mitigation measures.

## How to use this recommendation

### The risk assessment process is divided in 3 steps:

### Collect information on systems, equipment and connections, in order to define a

scope for the risk assessment. This should be complemented by architectural drawings in order to have a better understanding of the systems/equipment interconnections.

* Assess different systems parameters, either by relying on preassessed grades

published in this document or by applying the proposed risk assessment methodology. The combination of these parameters finally leads to a “risk level” grade for each system of the scope.

* Depending on the previously assessed “risk level” grade, decide or not to treat the risk, by defining and implementing relevant mitigation measures, until the “residual” risk level is considered acceptable and assumed as such.

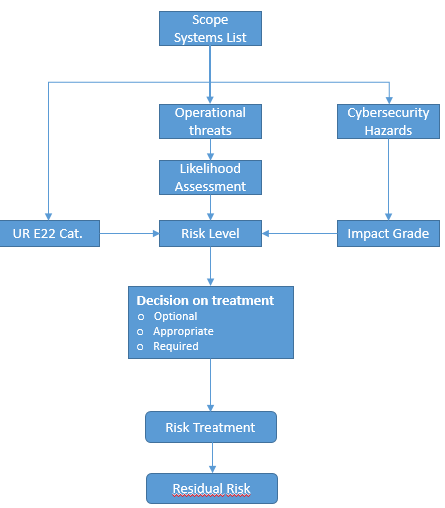
### The cyber security risk assessment process must be conducted by competent people to be identified by Companies. Most ship owners have these resources. Those who do not have them will have to use service companies or consultants. It is important to be able to appreciate the different systems, equipment or network that serve the different functions of the ship (navigation, machine, loading, crew, passenger, communications), and the way they are interconnected, when relevant.

### Even if different types of ships (bulk carriers, container ships, crude oil tankers, chemical tankers, LNG & LPC carriers, RoRo, passenger ships, tugboats…) might have different specificities, this recommandation caters for these differences by adjusting the assessment grades on systems/equipment.

## Methodology

The risk assessment applies for a set of IT/OT systems (system list) that is to be defined.

A step-by-step process is then implemented on this list of systems in order to determine, for each system, a “risk level” grade.



## Reference Guidelines and Standards

### The following list provides references to international or industrial regulation that may be

### considered as a primary technical background for this recommendation

* ISM Code
* IMO Resolution MSC.428(98) on maritime cyber risk management in safety management systems
* MSC-FAL.1/Circ.3 (5 July 2017) “Guidelines on maritime cyber risk management”
* IACS Recommendation 166 on Cyber Resilience

# Terms and Definitions

### Availability

Availability of a system or equipment is the probability that it is not in a failed state at a point in time.

### Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

### Connectivity

A grade measuring the exposure of system interfaces and interconnections to distant cyberattacks.

### Complexity

A grade assessing the operability, management and administration of a system.

The higher the complexity grade, the higher the likelihood of a cyber threat against that system.

### Impact

A rating quantifying, for each system, the potential consequences on vessel operations of a cyberattack. The higher the impact rating, the higher the consequences of a cyber threat.

### Integrity

Data integrity is the maintenance of, and the assurance of, data accuracy and consistency.

Likelihood

A rating quantifying the chances that a cyber attack/incident will happen.

Residual Risk

The risk remaining after dedicated mitigation measures are implemented and effective.

### System

Combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes.

# Scope of application

Any system may be built of operational technology (OT) as well as information technology (IT). It may also be connected to and/or integrated with the shore side, including public authorities, marine terminals and cargo handlers.

The following scope of systems to be assessed is detailed in the below table, that must be amended/completed as much as necessary to perfectly reflect the OT/IT architecture of the considered ship.

Table 1 – Systems reference table

| SYSTEM | Purpose / Structure |
| --- | --- |
| Machinery Systems |
| Main Engine | All subsystems and equipment that are part of the ship's main propulsion |
| Remote Propulsion control system | All subsystems and equipment that allow remote control of the propulsion (e.g. bridge control of the variable pitch propeller, engine RPM or bow thrusters) |
| Engine Control System | All subsystems and equipment that allows to control ship’s engine |
| Boiler Management system | All subsystems and equipment that ensure safe start-up, operation and shut-down of process burners.  The system is designed to maintain an appropriate air/fuel mixture under varying load conditions and within safe limits. The system ensures near complete combustion of the fuel as efficiently as possible. |
| Steering Gear | The steering system usually consists of: a steering gear, a control equipment, a rudder carrier, a rudder and a rudder horn. |
| Auxiliary Engine | Auxiliary engine used for power generation, with its own local control unit. |
| Emergency generator control and safety system | A set of systems that provide the ship with backup power. |
| IAS  (Integrated Automation System) | The IAS consolidates the functions of monitoring and alarming of all automation systems on the ship. It is typically a distributed system, constituted of several substations connected to each other. |
| Ballast / Bilge Systems |
| Ballast water management system | Ballast water management system controls the pumping in, treatment and release of ballast water. |
| Remote Tank gauging system | Any subsystem and equipment whose basic function is to monitor the level of liquid in the vessel’s tanks. |
| Cargo Management Systems |
| Cargo Control and monitoring system  (loading computer) | Controls the loading/inloading processes within the ship stability and strength operating enveloppe. |
| Oil discharge monitoring and control equipment (ODME) | System used to monitor the oil content in the water discharged overboard below 15 ppm. |
| Inert Gas System | System used to lower the oxygen content of the gaz remaining in cargo tanks of oil tankers, LPG/LNG carriers. |
| Radio Communication Equipment |
| VHF (Very High Frequency) radio installation | System including several radio equipment allowing to communicate by voice up to a theoretical radius of 30 nautical miles. |
| MF/HF (Medium Frequency/ High Frequency) radio installation  MF radio installation | System including several radio equipment allowing to communicate by voice up to a theoretical radius of 200 nautical miles |
| INMARSAT-C | Recognized mobile satellite service ship earth station |
| NAVTEX receiver | System used to receive messages like navigational warnings and SAR information |
| Other satellite communication system | SATCOM regroups maritime broadband systems, providing simultaneous data and voice communication via satellite through the BGAN (broadband global area network). |
| Bridge Systems |
| Gyro compass | Non-magnetic compass based on a fast-spinning disc and the rotation of the Earth to find geographical directions automatically |
| ECDIS (Electronic Chart Display and Information system) | Geographic information system used for nautical navigation as an alternative to paper nautical charts |
| Speed Log | A system linked with an electronic instrument that measures the speed through water |
| Echo Sounder | Type of sonar used to determine the depth of water by transmitting sound waves through water. |
| AIS (Automatic Identification System) | Automated tracking system that exchanges and displays identification information with other vessels in the vicinity.  The AIS must be switched on at all times unless the Master deems that it must be turned off for security reasons. |
| GNSS receiver | Satellite-based Global Positioning System. |
| RADAR | Marine radars are X band or S band radars, used to detect other ships and land obstacles, to provide bearing and distance for collision avoidance and navigation at sea. |
| SSAS | Ship Security Alert System (SSAS) is a system that contributes to strengthen maritime security and suppress acts of terrorism and piracy against shipping.  In the event of attempted piracy or terrorism, the ship’s SSAS beacon can be activated, and appropriate law-enforcement or military forces can be dispatched. |
| BNWAS | A Bridge Navigational Watch Alarm System is an automatic system which sounds an alarm if the watch officer on the bridge of a ship falls asleep, becomes otherwise incapacitated, or is absent for too long.  The BNWAS is automatically engaged when the ship's autopilot is activated. |
| Heading or track control system. | Electronic device permitting the vessel to automatically maintain a set heading without need to tend the helm. Once a course is entered, the autopilot will maintain it by automatically adjusting the rudder. |
| VDR (Voyage Data Recorder) | A Voyage Data Recorder (VDR) collects data from all interfaced sensors on board the vessel, storing it in an external Data Recording Unit. |
| Weather Fax | Independent system providing weather information to ships at sea. The information is presented as a chart (map), showing barometric high pressures, low pressures, pressure gradients, wind speed and direction, and temperature. |
| Anemometer | Wind indicator used on ships and boats to point the direction of the wind. |
| Safety Systems |
| Fire detection system | Stand-alone fire detector system provide a visible and audible alarm on the vessel to indicate the occurrence and location of a fire.  The detectors throughout the vessel are wired to a fire control panel which provides visual and audible alerts and possibly alarms in other parts of the vessel as well. |
| Gas detection / Gas Sampling system | A system consisting of sensors that will alert crews in case of accidental leakage of hazardous gases from cargo storage tanks (typically for oil tankers and gas carriers). |
| Emergency Shut-down system | Deployed primarily on LNGCs, ESD system is intended to protect the vessel and the terminal (export or import) in the event of a loss of power, cryogenic hazards or fire.  It stops the flow of liquid and vapour in case of an emergency and puts the cargo handling system in a safe static state. |
| Other machinery Systems |
| Sewage treatment System | System treating the ship's wastewater |
| Incinerator | System designed to incinerate solid waste and all types of combustible, non-explosive oil sludge with a minimum flash point of 60°C, without being a nuisance to the environment. |
| Operation and User Systems |
| Gateway (firewall - router-switch) | Entry and exit point of the networks from board to shore.  The central gateway is used to connect and route the shipboard networks.  The gateway is often composed of other network and subsystem equipment that provide other services:  - Switches managing the transport of network packets.  - Computer firewall that ensures the security of network information by filtering ingress and controlling egress according to rules set by the administrator.  - Domain controller, which is the centerpiece of the Windows Active Directory service. It authenticates users, stores user account information and enforces security policy for a Windows domain. |
| Business  (operation’s network) | System and particular network composed of various network and software equipment.  They provide the ship with the applications and services necessary for its operational activity |
| Email System | Electronic messaging system linking ship and shore.  It usually consists of a specific application. |
| WIFI Router | Wireless access point with IEE 802.11n and 802.11b/g standards that allows remote connection to various networks. |

# Key ship board operations

In order to identify and evaluate key operations on board the ship, which are vulnerable to cyber-attacks, IACS UR E22 systems categories are used. System categories are assigned based on their effects on system functionality.

As a reminder, the three different categories are:

**Cat. I**

For those systems, failure will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

**Cat. II**

For those systems, failure could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

* Liquid cargo transfer control system,
* Bilge level detection and associated control of pumps,
* Fuel oil treatment system,
* Ballast transfer valve remote control system,
* Stabilization and ride control systems,
* Alarm and monitoring systems for propulsion systems.

**Cat. III**

For those systems, failure could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

* Propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship (devices used only during maneuvering are not in the scope of this requirement such as bow tunnel thrusters),
* Steering system control system,
* Electric power system (including power management system),
* Ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in operation of life saving appliances equipment,
* Dynamic positioning system of equipment classes 2 and 3 according to IMO MSC/Circ.645.

A category is proposed for each system in Table 3. Note that the exact category can be dependent on the risk assessment for all operational scenarios.

# Cyber threats, attacks and techniques

A list of cyber security threats, attacks and techniques is provided in table 2 (appendix 1).

This list is non exhaustive. The shipowner, in coordination with his OT/IT managers and supervisors, may introduce additional threats if needed.

When a system has a connectivy grade matching the one in the dedicated column from table 2, the threat, attack or technique (and its consequences should they occur) are to be taken into consideration during the impact assessment (addressed in next chapter).

# Cyber Risk Assessment methodology

Two essential phases of any risk assessment are the determination of the threats impact (how much would the incident/accident affect operations?) and the threats likelihood (as the name suggests, what are the chances such threats may occur?).

The cyber risk assessment methodology makes no exception. Once threats are identified, first phase will be the determination of the threats impact, and second phase will be focused on the threats likelihood.

Combination of impact, likelihood and UR E22 category will provide a Risk Level for a system/equipment.

## Impact Assessment

Table 3 in this chapter proposes to consider threats consequences in terms of availability, confidentiality, integrity and traceability for each system described in the Scope of Application of this document.

Table 3 only contains proposals for threats impacts on each system. These proposals should be challenged by the users of this recommendation. They can in no way be considered as a truth for all cases.

To challenge these impact proposals, it is advised to consider each threat from table 2 and think about the impact they may have, should they occur, on the system/equipment, and then check if the impact proposed in table 3 is consistent with the real environment of the ship and her owner.

Impact grades are defined as follows:

*Impact P1: Negligible*

Events with a negligible impact, such as one or more of the following:

* System could be shutdown without any significant effect,
* No human nor environmental impacts involved.

*Impact P2: Acceptable*

Events with an acceptable impact, such as one or more of the following:

* shutdown of the system means a pointed disrupt of the service,
* environmental impact is in the standard margin and has no consequence but to be declared to authorities,
* event could lead to labour disruption because of injuries and medical treatment.

*Impact P3: Moderate*

Events with moderate impact, such as one or more of the following:

* loss of system activity is significant (e.g. email system is off and IT department needs time to recover),
* shipowner request investigations from a third-party committee (e.g. unexplained disruption of business activity, loss of non-repudiation traceability),
* loss of confidential information (e.g. data leaks, competitive know-how disclosure),
* financial loss are considered unacceptable by the shipowner,
* fraud and money theft,
* cargo and goods robbery,
* tarnished reputation,
* environmental impact is limited,
* limited loss of competitiveness and financial impact,
* human impact leading to permanent disability.

*Impact P4: High*

Events with a high impact, such as one or more of the following:

* physical systems damages (e.g. material breakage),
* permanent loss of the system without standard restoration process (e.g. ransomware) to restart it in its operational state,
* ship is off (e.g. cargo management is off),
* the regulatory asks for investigation,
* illegal trafficking,
* significant pollution conducts to people evacuation,
* long-term loss of competitiveness,
* human impact leads to death.

*Impact P5: Catastrophic*

Events with a catastrophic impact, such as one of the following:

* physical systems destruction (e.g. fire, explosion),
* loss of the vessel (e.g. collision or grounding),
* fleet is put offline (e.g. systems blackout, legal investigations),
* environmental disaster (e.g. major pollution) with long-term environmental consequences,
* financial loss conducts to shipowner bankruptcy,
* human impact leads to multiple deaths or crew, passengers kidnapping.

Table 3 – Impact assessment table

In this table, when threats have different consequences on availability, confidentiality, integrity and traceability, only the highest impact grade (of the worst consequence) is kept.

| **SYSTEM** | **UR E22 CAT** | **Threats consequences in terms of availability, confidentiality, integrity**  **and traceability (when relevant)** | **MaximumImpact P** |
| --- | --- | --- | --- |
| Machinery Systems |
| Main Engine | CAT III | **Integrity:** Invalid order sent to any PLC may lead to ship loss.  **Availability:** Should not be impacted as the engine control is backed up by a local control in application of the SOLAS.  **Traceability:** In case of incident, lack of traceability of orders may lead to legal pursuits. | **5** |
| Remote Propulsion control system | CAT III | **Integrity:** Corruption of this system may lead to erratic maneuvre.  **Availability:** Unavailability of the system does not entail a major safety risk as the vessel remains controllable.  **Traceability:** In case of incident, lack of traceability of orders may lead to legal pursuits. | **4** |
| Boiler Management system | CAT II | **Integrity:** Data integrity with IAS must be guaranteed.  **Availability:** The system must remain available to ensure an acceptable level of security. | **3** |
|
| Steering Gear System | CAT III | **Integrity:** Corruption of data may lead to erratic maneuvre.  **Availability:** Loss of this system would lead to a situation where the vessel could no longer be maneuvred. | **4** |
|
|
| Auxiliary Engine | CAT III | **Availability:** The system must remain available to ensure safety and security. | **4** |
| Emergency generator control and safety system | CAT III | **Integrity:** A false order on a connected system may have safety consequences for the ship.  **Availability:** The unavailability of the system does not pose a major safety risk in the short term. If prolonged, it may impact operational business. | **3** |
| IAS  (Integrated Automation system)  (when IAS only collects information) | CAT II | **Confidentiality:** Loss of confidentiality has a limited impact, as no sensitive information is transmitted.  **Integrity:** false information on the status of shipboard systems can impact operational business.  **Availability:** if shore needs this information to plan short and medium terms business, then the impact is unacceptable, otherwise the impact is limited. | **3** |
| IAS  (when IAS interacts with the systems to which it is connected) | CAT III | **Confidentiality:** Loss of confidentiality from IAS systems has a limited impact, as no sensitive information is transmitted.  **Integrity:** Integrity must be guaranteed, in order to ensure  appropriate operational decisions.  **Availability:** If an administration link (update, remote monitoring) exists between ship and shore, then availability must be guaranteed.  In addition, if the shore needs IAS data on a regular basis in order to plan operational activities, loss of availability can become unacceptable.  **Traceability:** Traceability is essential to ensure that access to this system is monitored, and that actions are compliant with cyber rules on this system. | **4** |

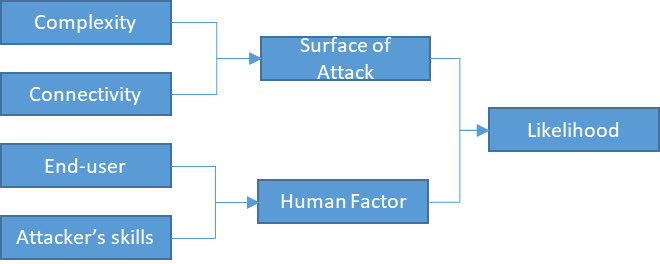
|  |
| --- |
| Ballast / Bilge Systems |
| Ballast water management system | CAT II | **Integrity:** Loss of integrity has a high impact, as a corrupt information can lead to the ship capsizing.  **Availability:** Loss of availability is unacceptable. It could strongly delay operational activity. | **4** |
| Remote Tank gauging system | CAT III | **Integrity:** Loss of integrity can lead to limited environmental impact.  **Availability:** Loss of availability is acceptable. There is no immediate danger to the environment. Short and medium term intervention has to be considered. | **3** |
| Cargo Control and monitoring system  (loading system) | CAT III | **Confidentiality:** Leak or corruption of sensitive business information is unacceptable.  **Integrity:** Loss of integrity may lead to major environmental pollution.  **Availability:** Loss of availability is unacceptable, as it can represent a hazard to crew members or considerably delay business activities.  **Traceability:** Must be guaranteed and ensured by authorized crew members with legit access to the registry information data. | **4** |
| Oil discharge monitoring and control system (ODME) | CAT III | **Integrity:** Loss of integrity can lead to limited environmental impact.  **Availability:** Loss of availability is acceptable, as there is no immediate danger to the environment. Short and medium term intervention has to be considered. | **3** |
| Inert Gas System | CAT III | **Integrity:** Loss of integrity increase the danger of explosion.  **Availability:** Loss of availability is unacceptable. There is no immediate physical danger. Intervention has to be considered in short and medium term. | **3** |
| Loading computer | CAT III | **Confidentiality:** Leak or corruption of sensitive information is unacceptable.  **Integrity:** Loss of integrity may lead to major environmental pollution.  **Availability:** Loss of availability is unacceptable, as it can represent a hazard to crew members or considerably delay business activities. | **4** |
| VHF | CAT III | **Availability:** Loss of communications, is acceptable off shore. But during land approach or in case of high traffic, permanent loss becomes acceptable. | **3** |
| MF/HF | CAT II | **Availability:** Loss of communications, is acceptable off shore. But during land approach or in case of high traffic, permanent loss becomes acceptable. | **3** |
| INMARSAT-C | CAT II | **Availability:** As it impacts emergency communication at sea, loss of availability is unacceptable. | **3** |
| NAVTEX Receiver | CAT II | **Integrity:** Loss of integrity may delay business activity - Unacceptable.  **Availability:** Loss of availability has a considerable impact on navigation safety - High | **4** |
| SATCOM / V-SAT | CAT I | **Confidentiality:** Leak or corruption of sensitive information is unacceptable.  **Integrity:** Loss of integrity is unacceptable, operational data integrity must be guaranteed.  **Availability:** Loss of availability is unacceptable, all IT data must be available at all times.  **Traceability:** Loss of traceability would make it impossible to justify any management action on the system. | **3** |
| SATCOM / FBB (Fleet Broad Band) | CAT I | **Integrity:** Loss of integrity is unacceptable, as it affects the safety of navigation**.**  **Availability:** Loss of availability is acceptable, as navigation can still be handled from the bridge. | **3** |
| Bridge System |
| Gyro compass | CAT III | **Integrity:** Loss of integrity can send wrong information to steering gear, which would have high impact on safety.  **Availability:** Loss of availability can affect the autopilot, but the impact is acceptable**.** | **4** |
| ECDIS (Electronic Chart Display Information system) | CAT III | **Integrity:** Corruption of data charts may considerably affect ship safety and security. High impact  **Availability:** Loss of availability may seriously affect ship safety and security. High impact | **4** |
| Speed Log | CAT II | **Availability:** Loss of availability does not affect the navigation safety. | **2** |
| Echo Sounder | CAT III | **Integrity:** Loss ofintegrity can disrupt safety of navigation. Unacceptable.  **Availability:** Loss of availability can disrupt safety of navigation. | **3** |
| AIS (Automatic Identification system) | CAT II | **Integrity:** As the system is used as an anti-collision tool, loss ofintegrity can disrupt safety of navigation. High**. Availability:** Loss of availability does not affect the navigation, as other anti-collision tools can be used. | **4** |
| GNSS receiver | CAT III | **Integrity:** Loss of integrity directly impacts the ship safety and security.  **Availability:** Loss of availability seriously disrupts safety of navigation. | **4** |
| RADAR | CAT III | **Integrity:** Loss of integrity, though unlikely, would seriously disrupt safety of navigation**.**  **Availability:** Loss of availability would seriously disrupt safety of navigation. | **4** |
| SSAS (Ship Secure Alarm system) | CAT III | **Availability:** Loss of availability is unacceptable, as ship cannot alert in case of pirat attack. | **3** |
| BNWAS (Bridge Navigational Watch Alarm System) | CAT II | **Availability:** Loss of availability is unacceptable, as it can affect navigation safety in case the bridge operator is not present or not vigilant enough. | **3** |
| Heading or track control system | CAT III | **Integrity:** Autopilot corruption may lead to erratic maneuver.  **Availability:** Unavailability of the system is acceptable. | **4** |
|
| VDR (Voyage Data Recorder) | CAT I | **Integrity:** Integrity of data is valuable for forensics in case of incident investigation.  **Availability:** same as integrity. | **2** |
| Weather Fax | CAT I | **Integrity:** Loss of integrity is unlikely and has little impact.  **Availability:** Loss of availability has little impact | **1** |
| Anemometer | CAT I | **Negligible for C, I, A,T** | **1** |
| Safety System |
| Fire detection system | CAT III | **Availability:** Loss of fire detection and alarm system can affect the vessel safety. | **4** |
| Gas detection / Gas Sampling system | CAT III | **Availability:** Loss of this system can affect the vessel safety. | **4** |
| Emergency shut-down system | CAT III | **Availability:** Loss of this system can affect the vessel safety. | **4** |
| Sewage treatment System | CAT II | **Integrity:** Loss of integrity may have a limited environmental impact.  **Availability:** Loss of this system may have environmental impact. Unacceptable. | **3** |
| Incinerator | Cat I | **Integrity:** Loss of integrity is unlikely and has little impact.  **Availability:** Loss of availability has little impact | **1** |
| User IT systems |  |  |  |
| Gateway (firewall - router-switch- Domain controller) | CAT III | **Confidentiality:** Loss of confidentiality can lead to sensitive data being intercepted.  **Integrity:** Loss of data integrity has high impact. All systems can be corrupted from the gateway. Encryption of data by a ramsomware (onboard or onshore) without standard restoration process is a major hazard.  **Availability:** Loss of this system is acceptable in short term. | **4** |
| Business (crew network) | CAT I | **Confidentiality:** Loss of confidentiality can lead to sensitive data being corrupted, intercepted or disclosed. Unacceptable.  **Integrity:** Data encryption by ransomware is a major hazard.  **Availability:** Loss of this system can impact vessel or shipowner business.  **Traceability:** In case of data loss, lack of traceability or log history may lead to legal pursuits. | **3** |
| EMAIL SYSTEM | Cat I | **Confidentiality:** Loss of confidentiality can lead to sensitive data being corrupted, intercepted or disclosed. Unacceptable.  **Integrity:** Data encryption by ransomware is a major hazard.  **Availability:** Loss of this system can impact vessel or shipowner business.  **Traceability:** In case of data loss, lack of traceability or log history may lead to legal pursuits. | **3** |
|
|
| WIFI Router | CAT I | **Confidentiality:** Loss of confidentiality can lead to sensitive data being corrupted, intercepted or disclosed. Unacceptable.  **Integrity:** Data encryption by ransomware is a major hazard.  **Availability:** Loss of this system can impact vessel or shipowner business.  **Traceability:** In case of data loss, lack of traceability or log history may lead to legal pursuits. | **3** |

Note: Systems which are out of scope of UR E22 or whose categories are not specified in UR E22, categories only valid for the risk assessment mentioned in this Recommendation are indicated for convenience."

## Likelihood Assessment

For each system, a Likelihood grade can be assessed by combining parameters such as connectivity (CY), complexity (CX) and parameters taking into consideration human factors such as the user’s maturity level (end-user), and the attacker’s skill/motivation.

The likelihood assessment methodology is based on the following workflow:



### Complexity (CX) grade assessment

The complexity grade for each system is evaluated by using the following criteria:

CX1: Standalone Systems

Any system that requires little or no configuration change to operate (all updates and corrective maintenance excluded). E.g.: workstations

CX2: Living Systems

Living systems are systems or equipment for which software, configuration files or operating systems are modified or updated daily. E.g. any identification and authentication servers, database management systems, network equipment, any virtual machine monitors, calculators, any smart equipment used to take decision having a direct effect on vessel operations…

CX3: Distributed Systems

Distributed systems refers to systems the operability and efficiency of which require equipment distributed through remote or distributed architecture. E.g. unmanned vessels, swarm robotics,

distributed system architectures.

### Connectivity (CY) grade assessment

Connectivity grade qualifies the degree of connectivity of the system. The evaluation is performed using the following criteria

CY1: Isolated System

Any system that has no connection with any other system on board or on shore.

CY2: Closed connectivity System

Any system that shares one or more interconnection for exchange data only. These interconnections are made within the ship in a closed environment using protocols such as: NMEA, Modbus, dry contact, Serial...

CY3: Network System

Any system sharing at least one Ethernet, optical, wifi interconnection internal to the vessel, or any external connection using a proven managed and authenticated security protocol.

CY4: DMZs

Any system with a link external to the ship (e.g. gateway, remote administration link, web service, etc.) implementing an authenticated network link like classical VPN (VPN PPTT, SSL and TLS) where for any internet connection a DMZ-type architecture is deployed.

CY5: Open Connectivity Systems

Any system with an external link to a public network access, or without knowledge of special protection.

### Surface of attack (SA) grade assessment

Surface of attack grade is determined for each system by combining Connectivity (CY) and Complexity (CX) grades, using the following table.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | CY1 | CY2 | CY3 | CY4 | CY5 |
| CX1 | SA1 | SA2 | SA3 | SA4 | SA5 |
| CX2 | SA2 | SA2 | SA3 | SA4 | SA5 |
| CX3 | SA3 | SA3 | SA4 | SA4 | SA5 |

### End-Users (US) grade assessment

The grade of the end-users (US) ranges from US1 to US4 taking into account relevant crew (those who actually use the system/equipment) level of training/awareness, and the accessibility conditions of the system. A low level reduces the probability of a cyberattack.

The assessment of this grade takes into account not only the qualifications and awareness of the end-users, but also the physical/logical access controls applied to the system, as defined hereafter:

US1: Aware User

|  |  |  |
| --- | --- | --- |
| Cybersecurity Training/Awareness | Physical Access protection | Logical access protection |
| The crew is aware, well trained and knows how to implement cyber security measures for the system. | The room is locked by a physical barrier (keylock, code, badge, etc.) and access is only allowed by accreditation from the company or the Master. | The user has got a dedicated account and private password. |

US2: Controlled User

|  |  |  |
| --- | --- | --- |
| Cybersecurity Training/Awareness | Physical Access protection | Logical access protection |
| The crew is aware about cyber security, but poorly trained on cyber measures implementation. | The room is locked by a physical barrier (keylock, code, badge, etc.) and access is only allowed by accreditation from the company or the Master. | The user has got generic access (by his function) and generic password |

US3: Accredited User

|  |  |  |
| --- | --- | --- |
| Cybersecurity Training/Awareness | Physical Access protection | Logical access protection |
| The crew is very poorly trained and aware about cyber security issues and measures. | Access is allowed by accreditation from the company or the Master. | No |

US4: Any User

|  |  |  |
| --- | --- | --- |
| Cybersecurity Awareness | Physical Access protection | Logical access protection |
| Nothing is planned by Company related to cyber security training or awareness. | No | No |

### Attackers level (AT) grade assessment

The Attacker’s level (AT) is ranging from AT1 to AT5, depending on the level of competence expected from an attacker on the contemplated system. The grade should be selected in accordance with the following definitions.

AT1: Unintentional Attacker

Crew members having unintentionally and accidentally introduced on board a common, not targeted virus or malware.

AT2: Insider Attacker

Definition limited to crew members trying to bypass system security without malicious intention (e.g. equipment tuning, tinkers, and ethical hackers).

AT3: Standard Attacker

Any attacker (internal or external) with malicious intent using hacking tools and techniques. This level can be applied by default.

AT4: Criminal Attacker

Criminal attackers are considered as willing to invest time and money to gather intelligence about the shipping company, the fleet and the vessels. They will probably build a dedicated scenario to penetrate the system in order to install an Advanced Persistent Threat (APT).

AT5: Cyber warfare Attacker

Attackers are considered using governmental attacks. This grade is to be applied for naval ships.

### Human Factor (H) grade assessment

The Human Factor grade is assessed by combining Users (US) and Attackers Level (AT) grades in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | US1 | US2 | US3 | US4 |
| AT1 | H0 | H1 | H1 | H2 |
| AT2 | H1 | H1 | H2 | H2 |
| AT3 | H1 | H2 | H2 | H3 |
| AT4 | H2 | H2 | H3 | H3 |
| AT5 | H2 | H3 | H3 | H4 |

## Likelihood Grade Assessment (L)

The Likelihood grade is obtained by combining Surface of Attack (SA) and Human factor (H) grades in the following table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | H0 | H1 | H2 | H3 | H4 |
| SA1 | L1 | L2 | L3 | L4 | L5 |
| SA2 | L2 | L3 | L4 | L5 | L6 |
| SA3 | L3 | L4 | L5 | L6 | L7 |
| SA4 | L4 | L5 | L6 | L7 | L8 |
| SA5 | L5 | L6 | L7 | L8 | L9 |

Likelihood with grade 1 to 4 is considered “Low”.

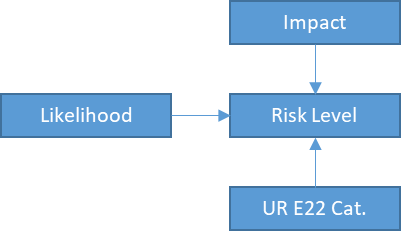
Likelihood with grade 5 to 7 is considered “Medium”

Likelihood with grade upper to 7 is considered “High”.

## Risk Level (RL) grade assessment

A risk level is assessed for each system in the scope.

The risk level is determined by using a formula integrating three main criteria which have been previously determined : Likelihood, Impact, UR E22 Cat.



The risk level grade (RL) is defined as:

Where:

* Cat denotes the Category number assigned to the contemplated system as per the IACS UR E22 definitions,
* L and P are respectively the Likelihood and Impact grades previously assessed.

The higher the risk level, the more mitigation measures might be required.

Risk level grade cannot be less than 1.

## Risk treatment

Depending on the risk level grade, risk treatment measures may be called, under appreciation of the cyber security responsible and his hierarchy.

RL< 4: risk treatment is considered “optional”.

4 ≤ RL ≤ 12: risk treatment is considered “appropriate”.

RL > 12 : risk treatment is considered “required”.

**7.6 Residual Risk Level (RRL)**

When risk treatment is “appropriate” or “required”, mitigation measures are to be considered. The purpose of these mitigation measures is to reduce the Risk Level to an acceptable level assumed by the shipowner, called “Residual Risk Level”.

Mitigation measures and their effects on Risk Levels are described in the following section.

# Mitigation measures

Mitigation measures range from the simplest and easiest to implement (so-called “human related” or "non technical" measures), to the most elaborate "technical" measures.

The desired level of effort depends on the Residual Risk Level to be achieved.

The higher the Risk Level of a system/equipment, the more mitigation measures might be required, and the greater the technical effort (and associated investment).

Mitigation measures should be chosen and implemented until an acceptable (and assumed by shipowner) Residual Risk Level is achieved.

Whatever mitigation measures are implemented, Residual Risk Level can not be less than 1.

**8.1. Non technical mitigation measures**

8.1.1. Human related mitigation measures

It cannot be stressed enough how important it is to raise the awareness and vigilance of crews regarding cyber security. Crew training may look like a simple and inexpensive measure to implement, yet it represents the smartest investment in this area.

Appendix 2 proposes contents for cyber security awareness and training.

Note that section 3.6.3. of BIMCO “Cyber Security Workbook for on board ship use” proposes a crew training cyber security checklist as well.

Ensuring regular vigilance training is a simple and effective mitigation measure.

When human related mitigation measures are applied, the previous RISK LEVEL can be reduced by 1.

*RRL = RL - 1*

8.1.2. Organisational mitigation measures

Ensuring that procedures are well described, efficient and available on board for systems/equipment monitoring, maintenance and incident response is a requirement of the ISM Code.

Ensuring that relevant personnel are fully aware of these procedures, and that they can implement them, is again a simple and effective mitigation measure.

Appendix 3 “items to be addressed in a cyber security risk management” proposes a list of organizational measures, not always related to procedures, but that are recommended to be implemented.

Note that already mentioned BIMCO Guidelines and Workbook represent high quality guides to put into practice an efficient cyber security risk management, as requested by IMO Resolution MSC.428(98).

When organisational measures are applied, the previous RISK LEVEL can be reduced by 3.

*RRL = RL - 3*

**8.2. Technical mitigation measures**

When organisational measures are not enough to reach an acceptable Residual Risk Level, technical mitigation measures are to be decided and implemented.

IACS Recommandation 166 on cyber resilience provides guidance for mitigating the risks

related to events affecting onboard computer-based systems. As a possible guidance, table 4 (in appendix 4) shows which sections of this Recommendation should be consulted when building a response to which type of attack or threat.

8.2.1. Technical “monitoring” solutions

Shipowner can decide, in coordination with his OT/IT managers and supervisors, to have a monitoring solution installed on board. Many technical monitoring solutions, such as real-time threat detection, intrusion prevention system, network security monitoring softwares, managed detection and response…, are already on shelves.

When a technical monitoring solution is installed as a mitigation measure, the previous RISK LEVEL can be reduced by 6.

*RRL = RL - 6*

8.2.2. Technical “hardening” measures

Shipowner can decide, in coordination with his OT/IT managers and supervisors, to install a

cyber security component (such as a Data Diode or a DMZ), or use certified equipment.

When a technical monitoring solution is installed as a mitigation measure, the previous RISK LEVEL can be reduced by 7.

*RRL = RL – 7*

**8.3. Combination of non technical and technical mitigation measures**

When one mitigation measure is not enough to reach an acceptable Residual Risk Level, shipowner can decide, in coordination with his OT/IT managers and supervisors, to implement a mix of non technical and technical measures.

When a combination of at least one non-technical mitigation measure and at least one technical mitigation measure are decided and implemented , the previous RISK LEVEL can be reduced by 9.

*RRL = RL – 9*

**APPENDIX 1**

Table 2 – Threats, attacks and techniques reference table

| Threat  Categories | Cyber threat, attack or technique | Definition | System  Connectivity |
| --- | --- | --- | --- |
| Nefarious activity/ abuse | Brute force | This attack is used to gain unauthorized access to an organization’s resources (such as data, systems, devices…) through many attempts to guess the correct key or password | CY2, CY3 |
| Denial of service DOS | The attacker leads to systems unavailability and production disruption. Most DoS attacks are caused by several sources at the same time (e.g. massive number of requests sent by different systems at the same time) sent to the target system, also called Distributed Denial of Service. | CY2, CY3 |
| Malware | The penetration of malicious software in the ship systems can lead to unwanted and unauthorized actions, exploiting some of their vulnerabilities to elevate the privileges and cause damage on ship IT/OT systems, infrastructure, data integrity and operations. For example, the most common malware in 2019, ransomware, could lead to ship paralysis by spreading onboard. | CY2, CY3 |
| Social engineering | The attacker can use human interactions to obtain or compromise information about ship organization and processes by asking questions, by pretending to be another person and piecing together information he needs. The attacker can ask several sources by relying on information he can get from the fist source to add to his credibility or send malicious links. | CY3 |
| Manipulation data | A manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information), e.g. malicious altering of electronic charts update. | CY2, CY3 |
| Phishing | The phishing attacks is the most common social engineering attack. Hackers use email or malicious websites to solicit personal information by posing as a trustworthy organization/person. | CY3 |
| Geo-localization spoofing | The hacker can manipulate geo-localization and navigation systems to change the ship trajectory and provoke shipwreck. GPS spoofing and AIS tampering are recent real attacks. | CY3 |
| Targeted attacks | A sophisticated and malicious attack specifically targeting a ship or a fleet, designed to infiltrate its systems for different purposes, such as data tampering. | CY3 |
| Abuse and theft of data | The hacker, through different means, steals sensitive data (personal data, freight tracking data, operational data…) and/or abuse the certificates used in the ship operations. | CY2, CY3 |
| Network manipulation and information gathering | The attacker scans the network passively until he can find an entry door which reveals to him internal ship network information (open ports, used protocols…). With this knowledge, the attacker operates to compromise the targeted systems. Example: a passenger gets access to passenger ship private network and initiates an evacuation alert for fun. | CY2, CY3 |
| Man in the middle | The attacker relays and possibly alters the communication between two parties who believe they are directly communicating with each other. | CY2, CY3 |
| Physical attacks | Sabotage | An action realized to deteriorate or destroy the ship systems and/or infrastructure. It can be external (from people not directly involved in the vessel operations) or internal (resentful employees…). Example: a container loading plan is altered by an activist who gets access to a crew member workstation. The container loading is incorrect, the cargo will be lost at sea, or break the hull or alter ship stability. | CY1 |
| Unauthorized physical access / unauthorized entry to premises | Unapproved access to sensitive equipment or data. | CY1 |
| Unintentional damage or error leading to loss of information or IT assets | Erroneous use or erroneous administration of devices and systems | Erroneous administration can strongly jeopardize ship systems proper functioning. | All CY |
| Erroneous penetration testing | In order to test ship IT or OT security level, the shipowner may order penetration tests which, if not carried out properly, can damage the systems. | All CY |
| Use of unreliable source | Defective updates or infected software. This may happen when patch or update management is insufficient. | All CY |
| Deletion/change of data in an information system | Loss of information integrity due to human error | All CY |
| Inadequate design and planning or improper adaptation | Threats caused by improper IT Assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors). | All CY |
| Third party security failure | If service providers are not correctly managed and controlled, their security breaches can directly affect the ship systems (in case of maintenance for instance). | All CY |
| Information leakage | Employees can share, by mistake or ignorance, sensitive data if there is an insufficient awareness or data protection solutions. | All CY |
| Malfunctions/Failures | Failures or malfunctions of devices or systems | When proper maintenance and compliance with manual/policy are not ensured, or when the proper functioning is not monitored correctly. | All CY |
| Vulnerabilities of systems or devices | Vulnerabilities that can exploited by hackers, particularly if those systems or devices are not properly monitored or maintained | CY2, CY3 |

**APPENDIX 2**

Recommandations on Crew Cyber Security Training and Awareness

Each crew member is essential in the cyber security protection chain. The way in which they have been made aware of cyber security issues, the basic rules to respect and the right behaviors to adopt, will be decisive. A lack of training or awareness, or a failure to assume one's responsibilities in terms of cyber security, represent vulnerabilities that can be exploited by an attacker. This should be a major concern of top management.

As recommended in chapters 6.2, 6.3 and 6.5 of the ISM Code, awareness actions are aimed at any person on board and potential user of one or several IT and/or OT information systems on board. They aim to provide basic and general knowledge in order to raise awareness on the issue of cyber security (and in particular to alert on bad practices).

The training actions are aimed at acquiring a more precise knowledge or know-how related to the same issue and are adapted to the appropriate levels for the personnel on board, in particular the cyber security responsible (whoever he is), but also the Master, Officers and Crew, as well as the port staff and any other shore personnel supporting the management, loading and operation of the vessel (IT and OT administrators, etc).

The following is not a comprehensive list, and should be adapted to the Company’s environment. The training should address at least the next points:

* Information system security objectives and issues;
* Vigilance over information considered sensitive;
* Legal and regulatory obligations;
* Compliance with shipowner cyber security rules;
* Implementation of Cyber Security safeguards and procedures
* Implementation of Cyber Security performance indicators for the safeguards
* Implementation of monitoring procedures
* Implementation of maintenance procedures
* Implementation of procedures related to reports and analysis of non-conformities, accidents and hazardous occurrence
* Importance of not connecting personal equipment (e.g. smartphone, USB key) to the company network on board;
* Careful use of passwords (no disclosure to unauthorized persons, necessity of “strong passwords”);
* Technical means involved in the security of the systems;
* Systematic locking of the session when the user leaves the computer;
* Implementation of password protection rules;
* General cyber security terminology and categorization;
* Malware, viruses and spyware;
* Identification of theft and compromise of classified data;
* Phishing and other dangers associated with emails (dangerous attachments, hoaxes, etc.);
* Risks regarding removable media, with focus USB stick dangers;
* Risks related to the presence of passengers on board;
* Locking of IT/OT rooms in passenger areas;
* Dangers of unsecured wireless networks;
* Desktop security;
* Social engineering/networking with an emphasis on the need for private and professional discretion on social networks or discussion forums;
* Risks associated with information, communication, navigation and automation systems on board

**APPENDIX 3**

**TOPICS WHICH SHOULD BE CONSIDERED WHEN DEVELOPING THE PROCEDURES**

The following topics should be considered when developing the procedures to be inserted into Safety Management System. This list is not exhaustive, and must be adapted to shipowner specificities and environment.

CYBER SECURITY MANAGEMENT

- Board level responsibilities. How does top level management gain information related to Cyber Security in the Company

- Who’s responsible for global (OT/IT) cyber security ashore? Main functions.

- Who’s responsible for global OT/IT cyber security on board (if any)? Main functions

- Who’s responsible for OT cyber on board? Main functions

- Who’s responsible for IT cyber on board? Main functions

- Main cyber responsibilities for crew members accessing OT/IT equipment

- Third parties management and main responsibilities

- Remote users management and main responsibilities

TRAINING AND AWARENESS

- What topics must it cover?

- Who’s in charge? Who organizes it?

- Who keeps traces of trainings?

- Social media policy

- Cyber security drills: periodicity, responsibilities, contents, feedback chain

INFORMATION MANAGEMENT AND PROTECTION

- Information evels of protection and sum-up of dedicated rules

- Regulatory requirements (GDPR if relevant)

- Use of e-mail (including categories of e-mail prohibited)

- Cyber doc update responsibilities

CHANGE MANAGEMENT PLAN FOR OT/IT SYSTEM/EQUIPMENT

- When is it to be used?

- Change request

- Change approval

- Change validation

PHYSICAL & LOGICAL SECURITY

- Vessel physical security – What parts of Ship Security Plan (SSP) could be used for critical OT/IT equipment protection

- Physical access control

- Logical access control (accounts management)

- Removable & digital assets policy

- Use of personal devices

- Password policy (including rules for composing it)

- Malware detection (including list of reasons to begin investigation + antivirus policy + scanning policy)

- Wireless access control (when relevant)

NETWORKS MANAGEMENT

* OT/IT networks management and segregation
* Crew network (leisure) management
* Security of network devices
* Networks monitoring
* Internet access

SATELLITE COMMUNICATIONS (when relevant)

REMOTE ACCESS MANAGEMENT (when relevant)

CYBER OPERATIONS

- Monitoring policy (what is monitored, what is to be checked, log management when relevant)

- Maintenance policy (including updates management, patch management and software control)

- Incident response policy (cyber event detection, non-compliance response, incident reporting procedure, crisis management, back up and restore plans)

**APPENDIX 4**

Table 4

Which sections of IACS Rec.166 should be consulted

when building a response to which type of attack or threat.

| **General type of threats** | **Threats, attacks or technique** | **IACS Rec 166 References to be used** |
| --- | --- | --- |
| Nefarious activity | Brute force | 7.2 Communication and interfaces  7.3 Network  7.3.1 Equipment standards  7.3.4 Control, Monitoring and alarm  7.3.6 Network Protection Safeguards  7.3.7 Cyber incident detection safeguards  7.3.9 Protection devices  7.3.11 Cyber incident response measure |
| Denial Of Service (DOS) | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network (except 7.3.10) |
| Malware | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network (except 7.3.2 – 7.3.10)  7.4 Computer based system Physical access control  7.4.4 Equipment  7.4.6 Use of mobile devices and portable storage devices  7.4.7 Equipment to restrict physical access  7.5 Software Assurance  7.5.1 Design & Development Requirements  7.6 Remote Access  7.7 Data Quality  7.7.1 Data security  7.7.4 Data Storage  7.8 System Recovery |
| Social  engineering | 7.3 Network  7.3.6 Network protection safeguards  7.3.7 Cyber incident detection safeguards  7.3.9 Protection devices |
| Manipulation data | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network (except 7.3.2)  7.4 Computer based system Physical access control  7.4.4 Equipment  7.4.6 Use of mobile devices and portable storage devices  7.4.7 Equipment to restrict physical access  7.5 Software Assurance  7.5.1 Design & Development Requirements  7.6 Remote Access  7.7 Data Quality  7.7.1 Data security  7.7.4 Data Storage  7.8 System Recovery |
| Phishing | 7.3 Network  7.3.6 Network protection safeguard  7.3.7 Cyber incident detection safeguards |
| Geolocaliza-tion spoofing | 7.5 Software assurance  7.7 Data Quality (except 7.7.4)  7.8 System Recovery (except 7.8.2) |
| Targeted attacks | All chapter 7 |
| Abuse and theft of data | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.4 Computer based system Physical access control  7.5 Software Assurance  7.6 Remote Access  7.7 Data Quality  7.8 System Recovery |
| Network manipulation and information gathering | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.4 Computer Based System physical access control  7.5 Software Assurance  7.6 Remote Access  7.7 Data Quality  7.8 System Recovery |
| Man in the middle | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network (except 7.3.2)  7.4 Computer based system Physical access control  7.6 Remote Access  7.7 Data Quality  7.8 System Recovery |
| Physical attacks | Sabotage | 7.1 Asset identification  7.4 Computer Based System physical access control  7.8 System recovery |
| Unauthorized physical access / unauthorized entry to premises | 7.1 Asset identification  7.4 Computer based system Physical Access control  7.6 Remote Access  7.8 System recovery |
| Unintentional damage or error leading to loss of  information or IT assets | Erroneous use or  administration of devices and systems | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.3.4 Control, Monitoring and alarm  7.3.5 Segregation and segmentation of network  7.3.6 Network protection safeguards  7.3.8 Network and system Recovery Measures  7.6 Remote Access (from locations not onboard the ship) |
| Erroneous penetration testing | 7.2 Communication and interfaces  7.3 Network  7.3.2 Design requirements  7.3.4 Control, Monitoring and alarm  7.3.6 Network protection safeguards  7.3.8 Network and system recovery measures  7.6 Remote Access (from locations not onboard the ship) |
| Use of  unreliable source | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.3.4 Control, Monitoring and alarm  7.3.5 Segregation and segmentation of network  7.3.6 Network protection safeguards  7.3.7 Cyber incident detection safeguards  7.3.8 Network and system recovery measures  7.3.9 Protection devices  7.3.11 Cyber incident response measure |
| Deletion /change of data in an information system | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.3.4 Control, Monitoring and alarm  7.3.5 Segregation and segmentation of network  7.3.6 Network protection safeguards  7.3.7 Cyber incident detection safeguards  7.3.8 Network and system recovery measures  7.3.9 Protection devices  7.3.11 Cyber incident response measure  7.6 Remote Access (from locations not onboard the ship)  7.7 Data Quality  7.7.1 Data security  7.7.3 Secured and encrypted data  7.7.4 Data storage  7.8 System Recovery |
| Inadequate design and planning or improper adaptation | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.6 Remote Access (from locations not onboard the ship)  7.7 Data Quality  7.7.1 Data security  7.7.3 Secured and encrypted data  7.7.4 Data storage  7.8 System Recovery |
| Third party security failure | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.3.2 Design requirements  7.3.3 Installation requirements  7.3.4 Control, Monitoring and alarm  7.3.5 Segregation and segmentation of network  7.3.6 Network protection safeguards  7.3.7 Cyber incident detection safeguards  7.3.8 Network and system Recovery Measures  7.3.10 Integration  7.5 Software Assurance  7.6 Remote Access (from locations not onboard the ship) |
| Information leakage | 7.1 Asset identification  7.2 Communication and interfaces  7.3 Network  7.3.3 Installation requirements  7.3.4 Control, Monitoring and alarm  7.3.6 Network protection safeguards  7.3.7 Cyber incident detection safeguards  7.3.9 Protection devices  7.3.11 Cyber Incident Response measure  7.4 Computer based system Physical Access control  7.7 Data Quality |
| Mal-functions  Failures | Failure of mal-function of devices or systems | 7.2 Communication and interfaces  7.8 System recovery |
| Vulne-rabilities of systems or devices | 7.2 Communication and interfaces  7.5 Software Assurance  7.8 System Recovery |