ISM Technical Notice NO31/2020

Dated: 03.12.2020

SUBJECT:

CYBER RISK MANAGEMENT

Introduction

The present circular/guidance has been development based on the "*The Guidelines on Cyber Security Onboard Ships*", version 3.0, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, WSC and IUMI, 2018, giving guidance on the **most brief and hopefully friendly way** regarding the main elements of the:

- **Cyber Risk Management** (CRM)
- **Minimum measures** that all companies should consider implementing so as to **address cyber risk management in an approved SMS**

Please note that according to the above provisions, INSB Class Auditors shall review the proper establishment of the CRM and how this is addressed in the SMS during the annual verification of the company's Document of Compliance after 1 January 2021.

1. General

In 2017, the International Maritime Organization (IMO) adopted resolution **MSC.428(98)** on **Maritime Cyber Risk Management** in Safety Management System (**SMS**). The Resolution stated that an approved SMS should take into account **cyber risk management** in accordance with the **objectives and functional requirements of the ISM Code**. Cyber Management should be appropriately **addressed** in safety management systems **no later than the first annual verification of the company's Document of Compliance after 1 January 2021.**

Approaches to cyber risk management will be **company- and ship-specific** but should be guided by the requirements of relevant **national, international and flag state** regulations.

IMO developed **guidelines** (MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management) that provide **high-level recommendations** on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

Cybertechnologies have become **essential** to the **operation and management** of numerous systems critical to the **safety and security of shipping** and protection of the marine environment. However, the **vulnerabilities created by accessing, interconnecting or networking** these systems can lead to cyber risks which should be addressed.

2. Cyber security concepts

2.1 Information Technology (IT) and Operational Technology (OT)

OT systems control the **physical world** and **IT** systems **manage data**. OT systems differ from traditional IT systems.

OT is hardware and software that directly monitors/controls physical devices and processes. **IT** covers the spectrum of technologies for information processing, including software, hardware and communication technologies.

Traditionally OT and IT have been separated, but with the **internet, OT and IT are coming closer** as historically stand-alone systems are becoming integrated.

Disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment, and impede the ship's operation.

2.2 Cyber security and cyber safety

Cyber security is concerned with the protection of IT, OT, information and data from unauthorised access, manipulation and disruption.

Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

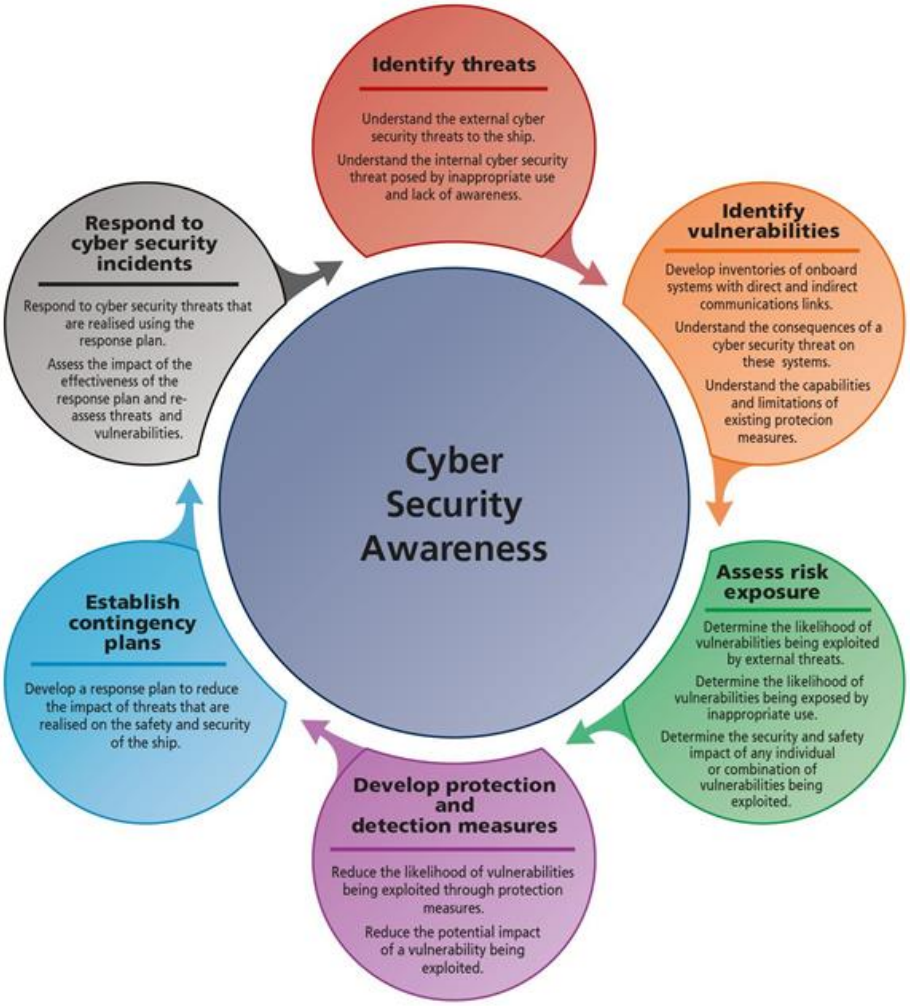
Cyber safety incidents can arise as the result of:

- a cyber security incident, which **affects the availability and integrity of OT**, for example corruption of chart data held in an Electronic Chart Display and Information System (**ECDIS**)
- a **failure** occurring during **software maintenance and patching**
- a **loss of or manipulation of external sensor data**, critical for the operation of a ship – this includes but is not limited to Global Navigation **Satellite Systems** (GNSS).

3. Cyber risk management

Cyber risk management should:

- identify the **roles and responsibilities** of users, key personnel, and management both **ashore** and **on board**
- **identify the systems, assets, data and capabilities**, which if disrupted, could pose risks to the ship's operations and safety
- implement **technical and procedural measures** to protect against a cyber incident and ensure continuity of operations
- implement activities to **prepare for and respond** to cyber incidents



Company needs to **assess risks arising from the use of IT and OT** onboard ships and establish appropriate **safeguards** against cyber incidents.

Company plans and **procedures for cyber risk management should be incorporated** into existing and safety risk management requirements contained in the **ISM Code and ISPS Code**.

The factors to be considered include but are not limited to the **extent to which IT and OT are used** on board, the complexity of system integration and the nature of operations.

3.1 Identify threats

There are **motives for organisations and individuals** to exploit cyber vulnerabilities. The following examples give some indication of the **threats posed and the potential consequences** for companies and the ships they operate:

Group	Motivation	Objective
Activists (including disgruntled employees)	▪ Reputational damage ▪ Disruption of operations	▪ Destruction of data ▪ Publication of sensitive data ▪ Media attention
Criminals	▪ Financial gain ▪ Commercial espionage ▪ Industrial espionage	▪ Selling stolen data ▪ Ransoming stolen data ▪ Ransoming system operability ▪ Arranging fraudulent transportation of cargo
Opportunists	▪ The challenge	▪ Getting through cyber security defenses ▪ Financial gain
States State sponsored organisations Terrorists	▪ Political gain ▪ Espionage	▪ Gaining knowledge ▪ Disruption to economies and critical national infrastructure.

Table 2: Motivation and objectives

In addition, there is the possibility that **company personnel, on board and ashore**, could compromise cyber systems and data. In general, the company should realise that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures.

Types of cyber attack
In general, there are two categories of cyber attacks, which may affect companies and ships:

Untargeted attacks,
where a company or a ship's systems and data are one of many potential targets

Targeted attacks,
where a company or a ship's systems and data are the intended target

3.2 Identify vulnerabilities

Company initially performs an **assessment of the potential threats** that may realistically be faced. This should be followed by an **assessment of the systems** and onboard **procedures** to map their robustness to handle the current level of threat.

Stand-alone systems will be less vulnerable to external cyber attacks **compared** to **those attached to uncontrolled networks or directly to the internet**. Care should be taken to understand how **critical shipboard systems might be connected to uncontrolled networks**. When doing so, the **human element** should be taken into consideration, as many incidents are initiated by personnel's actions.

3.2.1 Onboard systems could include:

- **Cargo management systems**
  Digital systems used for the loading, management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore, including ports, marine terminals.
- **Bridge systems**
  Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks. A cyber incident can extend to service denial or manipulation and, therefore, may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.
- **Propulsion and machinery management and power control systems**
  The use of digital systems to monitor and control onboard machinery, propulsion and steering makes such systems vulnerable to cyber attacks.
- **Access control systems**
  Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic "personnel-on-board" systems are vulnerable to cyber attacks.
- **Passenger servicing and management systems**
- **Passenger facing public networks**
- **Administrative and crew welfare systems**
  Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when providing internet access and email.
- **Communication systems**
  Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships.

3.2.2 Ship to shore interface

Ships are becoming more and more **integrated with shoreside operations** because digital communication is being used to conduct business, manage operations, and retain contact with head office.

Furthermore, **critical ship systems essential to the safety of navigation, power and cargo** management have become increasingly **digitalised and connected** to the internet to perform a wide variety of legitimate functions such as:

- engine performance monitoring
- maintenance and spare parts management
- cargo, loading and unloading, crane, pump management and stow planning
- voyage performance monitoring.

Common vulnerabilities
The following are common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships:

- **obsolete and unsupported** operating systems
- **outdated or missing antivirus** software and protection from malware
- **inadequate security configurations** and best practices, including ineffective network management and the use of default administrator accounts and **passwords**,
- shipboard **computer networks**, which **lack boundary protection** measures and segmentation of networks
- **safety critical equipment** or systems **always connected** with the shore side
- **inadequate access controls** for third parties including contractors and service providers.

3.3 Assess risk exposure

3.3.1 The following **questions** may be used as a **basis for a risk assessment** when addressing cyber risks onboard ships:

- What **assets** are at risk?
- What is the potential **impact** of a cyber incident?
- Who has the final **responsibility** for the cyber risk management?
- Are the **OT** systems and their working environment **protected** from the internet?
- Is there remote **access to the OT systems**, and if so how is it monitored and protected?
- Are the **IT systems protected** and is remote access being monitored and managed?
- What cyber risk management **best practices** are being used?
- What is the **training** level of the personnel operating the IT and OT systems?

3.3.2 The following should be addressed:

- **identify systems** that are important to operation, safety and environmental protection
- **assign the persons** responsible for setting cyber policies, procedures and enforce monitoring
- **determine where secure remote access** should use multiple **defence layers** and where protection of **networks** should be disconnected from the internet
- identification of needs for **training** of personnel.

3.3.3 Third-party access

Visits to ships by third parties requiring a **connection to one or more computers** on board can also result in connecting the ship to shore. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. Some technicians may require the use of removable media to update computers, download data and/or perform other tasks. It has also been known for customs officials and port state control officers to board a ship and request the use of a computer to "print official documents" after having inserted an unknown removable media.

Some IT and OT systems are remotely accessible and may operate with a continuous internet connection for remote monitoring, data collection, maintenance functions, safety and security.

Systems and work stations with remote control, access or configuration functions could, for example, be:

- **bridge and engine room computers** and workstations on the ship's administrative network

- **cargo** such as containers with **reefer temperature** control systems or specialised cargo that are tracked remotely
- **stability decision** support systems
- **hull stress** monitoring systems
- **navigational systems** including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP)
- **cargo handling** and stowage, engine, and cargo management and load planning systems
- safety and security networks, such as **CCTV** (closed circuit television)
- **specialised systems** such as drilling operations, blow out preventers, subsea installation systems, Emergency Shut Down (ESD) for gas tankers, submarine cable installation and repair.

3.3.4 Impact assessment

The **confidentiality, integrity and availability (CIA) model** provides a framework for **assessing the impact** of:

- **unauthorised access** to and **disclosure** of information or data about the ship, crew, cargo and passengers
- **loss of integrity**, which would **modify or destroy information** and data relating to the safe and efficient operation and administration of the ship
- **loss of availability** due to the **destruction of the information** and data and/or the disruption to services/ operation of ship systems.

A **risk assessment of OT systems needs to be based on an inventory** overview of equipment and/ or computer-based systems and a map of the networks' connections. Further, access points and communication devices should be part of this overview.

3.3.5 Risk assessment made by the company

The assessment should **assess the IT and OT systems** on board. When conducting the assessment, the company should consider the outcomes of the ship security assessment as well as the following:

1. identification of **existing technical and procedural controls** to protect the onboard IT and OT systems
2. identification of **IT and OT systems that are vulnerable including the human factor**, and the policies and procedures governing the use of these systems. The identification should include searches for known vulnerabilities relevant to the equipment as well as the current level of patching and firmware updates
3. identification and evaluation of **key ship board operations** that are vulnerable to cyber attacks
4. identification of **possible cyber incidents** and their **impact** on key ship board operations, and the **likelihood** of their occurrence to establish and prioritise protection measures.

Companies may **consult with the producers and service providers** of onboard equipment and systems to understand the technical and procedural controls that may already be in place to address cyber risk management.

3.3.6 Ship assessment

The goal of the assessment of a ship's network and its systems and devices is to **identify any vulnerabilities** that could **compromise** or result in either loss of **confidentiality**, loss of **integrity** or result in a loss of **operation** of the equipment, system, network, or even the ship.

These **vulnerabilities and weaknesses** could fall into one of the following categories:

- **technical** such as software defects or outdated or unpatched systems
- **design** such as access management, unmanaged network interconnections

- **implementation errors** for example misconfigured firewalls
- **procedural** or other user errors.

The activities performed during an assessment could include **reviewing the configuration of all computers, servers, routers, and cyber security technologies including firewalls**.

An aspect of on-ship assessment is **involvement of crew** of all levels; particularly the master, chief engineer and first mate.

3.4 Develop protection and detection measures

3.4.1 Defense in depth and in breadth

Connected OT systems on board should require **more than one** technical and/or procedural **protection** measure. Perimeter defenses such as **firewalls** are important for preventing unwelcomed entry into the systems, but this **may not be sufficient** to cope with insider threats.

This **defense** in depth approach encourages a **combination** of:

- **physical security** of the ship in accordance with the ship security plan (SSP)
- protection of **networks**, including effective segmentation
- **intrusion** detection
- periodic **vulnerability scanning** and testing
- **software whitelisting**
- **access and user controls**
- appropriate procedures regarding the use of **removable media and password policies**
- personnel's **awareness** of the risk and familiarity with appropriate procedures

3.4.2 Technical protection measures

The Centre for Internet Security (CIS) provides guidance on measures that can be used to address cyber security vulnerabilities. **Critical Security Controls** (CSC) include both technical and procedural aspects. The below mentioned **examples** of CSCs have been selected as particularly **relevant to equipment and data onboard ships**:

- Limitation to and control of network ports, protocols and services
- Configuration of network devices such as firewalls, routers and switches
- Physical security
- Detection, blocking and alerts
- Satellite and radio communication
- Wireless access control
- Malware detection
- Secure configuration for hardware and software
- Email and web browser protection
- Data recovery capability
- Application software security (patch management)

3.4.3 Procedural protection measures

Procedural controls are focused on how personnel use the onboard systems.

3.4.3.1 Training and awareness

Training and awareness should be tailored to the appropriate levels for:

- **onboard personnel** including the master, officers and crew
- **shoreside personnel**, who support the **management, loading and operation** of the ship.

An **awareness programme** should be in place for all onboard personnel, covering at least the following:

- risks related to **emails** and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site
- risks related to **internet usage**, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored
- risks related to the **use of own devices**. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment, to which they are connected
- risks related to **installing and maintaining software** on company hardware using **infected hardware** (removable media) or **software** (infected package)
- risks related to **poor software** and data security practices, where no anti-virus checks or
- authenticity verifications are performed
- safeguarding u**ser information, passwords** and digital certificates
- cyber risks in relation to the **physical presence of non-company personnel**, eg, where third-party technicians are left to work on equipment without supervision
- detecting **suspicious activity or devices** and how to report a possible cyber incident. Examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network
- awareness of the **consequences** or impact of **cyber incidents** to the safety and operations of the ship
- understanding how to implement **preventative maintenance routines** such as **anti-virus and antimalware**, patching, backups, and incident-response planning and testing
- procedures for protection against risks from **service providers' removable media** before connecting to the ship's systems.

Further, applicable **personnel** should know the **signs when a computer has been compromised.** This may include the following:

- an unresponsive or slow to respond system
- unexpected password changes or authorised users being locked out of a system
- unexpected errors in programs, including failure to run correctly or programs running unexpectedly
- unexpected or sudden changes in available disk space or memory
- emails being returned unexpectedly
- unexpected network connectivity difficulties
- frequent system crashes
- abnormal hard drive or processor activity
- unexpected changes to browser, software or user settings, including permissions.

3.4.3.2 Access for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives should be **restricted with regard to computer access** whilst on board. **Unauthorised access** to sensitive OT network computers should be **prohibited**.

3.4.3.3 Upgrades and software maintenance

Hardware or software that is **no longer supported** by its producer or software developer will not receive updates to address potential vulnerabilities.

Relevant hardware and software installations on board should be **updated** to help maintain a sufficient level of security.

3.4.3.4 Anti-virus and anti-malware tool updates

3.4.3.3 Remote access

Policy and procedures should be established for **control over remote access** to onboard IT and OT systems.

3.4.3.5 Use of administrator privileges

Access to information should only be allowed to relevant **authorised personnel**.

3.4.3.6 Physical and removable media controls

When transferring data from uncontrolled systems to controlled systems, there is a risk of introducing malware. **Removable media** can be used to bypass layers of defences and attack systems that are otherwise not connected to the internet.

Policies and procedures relating to the use of removable media should include a **requirement to scan** any removable media device in a computer that is not connected to the ship's controlled networks. If it is not possible to scan the removable media on board, eg the laptop of a maintenance technician, then the scan could be done prior to boarding.

3.4.3.7 Equipment disposal, including data destruction

3.4.3.8 Obtaining support from ashore and contingency plans

3.5 Establish contingency plans

When developing contingency plans for implementation onboard ships, it is important to understand the **significance of any cyber incident and prioritise response actions** accordingly.

Any cyber incident should be assessed to estimate the **impact** on operations, assets etc. In most cases, and with the exception of load planning and management systems, a **loss of IT** systems on board, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the ship.

In the event of a cyber incident affecting **IT systems only**, the priority may be the immediate implementation of an **investigation and recovery plan**.

The **loss of OT systems** may have a **significant and immediate impact** on the safe operation of the ship. Should a cyber incident result in the loss or malfunctioning of OT systems, it will be essential that effective actions are taken to help ensure the immediate safety of the crew, ship, cargo and protection of the marine environment.

In general, appropriate **contingency plans for cyber incidents**, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by the relevant operational and emergency procedures included in the **safety management system**.

The following is a non-exhaustive list of **cyber incidents, which should be addressed** in contingency plans on board:

- loss of availability of **electronic navigational equipment** or loss of integrity of navigation related data
- loss of availability or **integrity of external data sources**, including but not limited to GNSS
- loss of essential **connectivity with the shore**, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications
- loss of availability of industrial **control systems**, including **propulsion, auxiliary systems** and other critical systems, as well as loss of integrity of data management and control
- the event of a **ransomware** or denial or service incident.

3.6 Respond to and recover from cyber security incidents

3.6.1 Effective response

A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations.

An effective response should at least consist of the following steps:

1. **Initial assessment**. To help ensure an appropriate response, the response team should find out:
   - **how** the incident occurred
   - **which IT** and/or **OT** systems were affected and how
   - the **extent** to which the commercial and/or operational data is affected
   - to what **extent** any **threat** to IT and OT **remains**.

2. **Recover systems and data**. Following an initial assessment of the cyber incident, IT and OT systems and data should be **cleaned, recovered and restored**, so far as is possible, to anoperational condition by removing threats from the system and restoring software.
3. **Investigate the incident**.
4. **Prevent a re-occurrence**.

When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to **initiate the recovery plan** alongside onboard contingency plans.
When this is the case, the response team should be able to **provide advice** to the ship on:

- whether **IT or OT systems should be shut down or kept running** to protect data
- whether certain **ship communication links with the shore should be shut down**
- the appropriate **use of any advanced tools** provided in pre-installed security software
- the **extent** to which the incident has **compromised IT or OT** systems beyond the capabilities of existing HA recovery plans.

It is important for relevant personnel to **execute regular cyber security exercises** in order to help keep the response capability effective.

3.6.2 Recovery plan

Recovery plans should be available in **hard copy** on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state.

To help ensure the safety of onboard personnel, the **operation and navigation of the ship should be prioritised** in the plan. The recovery plan should be **understood by personnel** responsible for cyber security. The **detail and complexity** of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

3.6.3 Investigating cyber incidents

Investigating a cyber incident can provide valuable information about the way in which a vulnerability was exploited. Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board in accordance with company procedures. A detailed investigation may require external expert support.

4. Cyber risk management and the safety management system

The guidance provided in the IMO Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the 5 elements of an appropriate approach to implementing cyber risk management:

1. **Identify**: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
2. **Protect**: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
3. **Detect**: Develop and implement activities necessary to detect a cyber-event in a timely manner.
4. **Respond**: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
5. **Recover**: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

1. IDENTIFY

1.1 Roles and responsibilities

- **ISM Code: 3.2**: **Update the safety and environment protection policy** to include reference to the risk posed by unmitigated cyber risks.
- **ISM Code: 3.3**: **Update the responsibility and authority** information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).
- **ISM Code: 6.5:** Using existing company procedures, **identify any training** which may be required to support the incorporation of cyber risk management into the SMS.

1.2 Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

- **ISM Code: 10.3:** Using existing company procedures, **identify equipment and technical systems (OT and IT)** the sudden operational failure of which may result in hazardous situations.

2. PROTECT

2.1 Implement risk control measures

ISM Code: 1.2.2.2: Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.

The full scope of **risk control measures** implemented by the company should be determined by a **risk assessment**, taking into account the information provided in these guidelines.

As a baseline, the following **measures should be considered before a risk assessment** is undertaken. The baseline consists of the **technical and procedural measures**, which should be **implemented in all companies** to the extent appropriate.

These measures are:

2.1.1 Hardware inventory

Develop and maintain a **register of all critical system hardware** on board, including **authorized and unauthorized devices on company controlled networks**.
The SMS should include procedures for **maintaining this inventory** throughout the operational life of the ship.

2.1.2 Software inventory

Develop and maintain a **register of all authorized and unauthorized software** running on company-controlled hardware onboard, including version and update status.

The **SMS** should be updated to include **procedures** for:

- **maintaining** this **inventory** when **hardware** controlled by the company is **replaced**
- **maintaining** this **inventory** when **software** controlled by the company is **updated or changed**
- **authorizing** the **installation** of new or upgraded **software** on hardware controlled by the company
- **prevention** of **installation** of **unauthorized software**, and deletion of such software if identified
- **software maintenance**.

2.1.3 Map data flows

Map **data flows between critical systems and other equipment/technical systems on board and ashore**, including those provided by third parties. **Vulnerabilities** identified during this process should be **recorded** and securely retained by the company.

The **SMS** should be updated to include **procedures** for:

- **maintaining** the map of **data flows** to reflect **changes** in **hardware**, **software** and/or **connectivity**
- **identifying** and responding to **vulnerabilities** introduced when **new data flows are created** following the installation of **new hardware**
- **reviewing** the need for **connectivity** between critical systems and other OT and IT systems. Such a review should be based on the principle that **systems should only be connected where there is a need** for the safe and efficient **operation** of the ship, or to enable **planned maintenance**
- **controlling** the use of **removable media, access points** and the creation of ad-hoc or **uncontrolled data flows**. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems.

Implement secure configurations for all hardware controlled by the company
This should include **documenting and maintaining** commonly accepted **security configuration standards** for all authorized **hardware and software**.

The **SMS** should include policies on the **allocation and use of administrative privileges** by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company.

2.1.4 Audit logs

Security logs should be maintained and periodically reviewed. **Security logging** should be enabled on all **critical systems** with this capability.

The **SMS** should be updated to include **procedures** for:

- policies and procedures for the **maintenance of security logs** and periodic **review** by competent personnel as part of the operational maintenance routine
- procedures for the collation and retention of security logs by the company, if appropriate.

2.1.5 **Awareness and training** – as above.

2.1.6 Physical security

The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code.
Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.

2.2 Develop contingency plans

ISM Code 7: Update procedures, plans and instructions for **key shipboard operations** concerning the safety of the personnel, ship and protection of the environment **which rely on OT**

ISM Code 8.1: Update emergency plans to include responses to **cyber incidents**

3. DETECT

3.1 Develop and implement activities necessary to detect a cyber-event in a timely manner

ISM Code 9.1: Update procedures for **reporting non-conformities**, accidents and hazardous situations to include reports relating to **cyber incidents**.
Examples of such non conformities and cyber incidents:

- unauthorised access to network infrastructure
- unauthorized or inappropriate use of administrator privileges
- suspicious network activity
- unauthorised access to critical systems
- unauthorised use of removable media
- unauthorised connection of personal devices
- failure to comply with software maintenance procedures
- failure to apply malware and network protection updates
- loss or disruption to the availability of critical systems
- loss or disruption to the availability of data required by critical systems

4. RESPOND

4.1 Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event

ISM Code 3.3: Ensure that **adequate resources** and shore-based support are available to support the DPA in responding to the loss of critical systems.
Incorporation of CRM into the SMS should require that this **resourcing includes appropriate IT expertise.**

ISM Code 9.2: Update **procedures** for implementing **corrective actions** to include **cyber incidents** and measures to prevent recurrence.

ISM Code 10.3: **Update** the specific measures aimed at **promoting the reliability of OT**.
An approved SMS should already include **procedures for operational maintenance** routines to promote the reliability of equipment on board:

- **Software maintenance** as a part of operational maintenance routines
- **Authorizing remote access**, if necessary and appropriate, to critical systems for software or other maintenance tasks.
- **Preventing** the application of **software updates by service providers** using uncontrolled or infected **removable media**.
- Periodic **inspection of the information provided by critical systems** to operators and confirmation of the accuracy of this information when critical systems are in a known state.
- Controlled use of **administrator privileges** to limit software maintenance tasks to competent personnel.

5. RECOVERY

5.1 Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident

ISM Code 10.4: Include **creation and maintenance of back-ups** into the ship's operational maintenance routine.