# SIRE 2.0 Question Library
# Part 1 – Chapters 1 to 7
# Version 1.0

**(January 2022)**

**The Oil Companies International Marine Forum (OCIMF)**
Vision: A global marine industry that causes no harm to people or the environment.

Mission: To lead the global marine industry in the promotion of safe and environmentally responsible transportation of crude oil, oil products, petrochemicals and gas and to drive the same values in the management of related offshore marine operations. We do this by developing best practices in the design, construction and safe operation of tankers, barges and offshore vessels and their interfaces with terminals and considering human factors in everything we do.

## 7.5. Cyber Security

### 7.5.1. Were the Master and officers familiar with the company procedures for cyber security risk management, and had these procedures been fully implemented?

**Short Question Text**
Cyber security risk management.

**Vessel Types**
Oil, Chemical, LPG, LNG

**ROVIQ Sequence**
Documentation, Bridge, Cargo Control Room, Engine Control Room

**Publications**
OCIMF/ICS: International Safety Guide for Oil Tankers and Terminals. Sixth Edition.
IMO: ISM Code
IMO: MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management
Industry: The Guidelines on Cyber Security Onboard Ships Version 4
IMO: Resolution MSC.428(98) Maritime cyber risk management in safety management systems

**Objective**

**To ensure the vessel has in place effective technical and procedural measures to protect against a cyber incident and ensure continuity of operations.**

**Industry Guidance**

**OCIMF/ICS: International Safety Guide for Oil Tankers and Terminals. Sixth Edition**

6.4 Cyber safety and security

Cyber security is concerned with the protection of Information Technology (IT), Operational Technology (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.

**IMO: MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management**

2.1.2 The distinction between information technology and operational technology systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

**Industry: The Guidelines on Cyber Security Onboard Ships Version 4**

1.1 Cyber security characteristics of the maritime industry

...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, that if disrupted, could pose risks to the ship's operations and safety.
- Implement technical and procedural measures to protect against a cyber incident, timely detection of incidents and ensure continuity of operations.
- A contingency plan which is regularly exercised.

**TMSA KPI 13.1.2** requires that the company has documented procedures in place to identify security threats applicable to vessels trading areas and shore-based locations. Security threats may include:

- Cyber threat

The identified threats are reviewed as required by changes in circumstance.

**IMO: ISM Code**

8.1 The Company should establish procedures to identify describe and respond to potential emergency shipboard situations.

**IMO: Resolution MSC.428(98) Maritime cyber risk management in safety management systems**

The Maritime Safety Committee,

1 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;

2 Encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

**Inspection Guidance**

The vessel operator should have developed procedures for cyber risk management that:

- Identified the roles and responsibilities of users, key personnel, and management both ashore and on board, including:
  - The officer with responsibility for cyber risk management on board.
  - The person responsible for managing user profiles and passwords in the vessel network.
- Identified the IT(information technology) and OT(operational technology) systems at risk on board such as:
  - Cargo management systems.
  - Bridge systems.
  - Propulsion and machinery management and power control systems.
  - Access control systems.
  - Administrative and crew welfare systems.
  - Communication systems.
- Described technical protection measures to protect against a cyber incident such as
  - Physical security of network components.
  - Anti-virus software.
  - Application software management.
  - Back-up facilities.
  - Control of crew internet access.
  - Control of administrator profiles, user profiles and passwords.
- Described procedural protection measures to protect against a cyber incident such as:
  - Cyber security training and awareness raising for crew members.
  - Control of local and remote access to the IT and OT systems.
  - Control of the use of personal devices on board.
  - Equipment disposal including data destruction.
  - Contingency plans for possible cyber incidents.

Spaces containing sensitive IT or OT control equipment should be securely locked.

Physical access to sensitive user equipment (such as exposed USB ports on bridge systems and wi-fi hub ports) should be secured or disabled.

All on-board computers should be protected by anti-virus software, and this should be kept updated.

Only senior officers should have administrator profiles and the responsibility for maintaining user profiles should be clearly set out. User profiles should only allow workstations etc. to be used for their intended purpose. User profiles should be carefully managed, and redundant profiles deleted.

Generic user profiles and passwords should not be passed on as part of crew changes. Passwords should be changed regularly.

Back-up facilities should be available and used to assist recovery following a cyber incident.

OT systems critical to navigation and propulsion should have backup systems enabling quick and safe recovery after a cyber incident.

Application software should be regularly updated with security patches and upgrades.

Crew members should receive cyber security training as appropriate to their responsibilities and duties.

Cyber security awareness should be actively promoted on board using for example, posters, CBT or online courses.

Computer access for visitors such as surveyors, technicians etc. should be restricted. Unauthorised access to sensitive OT computers should be prohibited. There should be procedures for the approval of access to sensitive networks, including remote access.

Procedures should strictly restrict the use of portable media. Where use is unavoidable, such media should be checked for malware etc. in a computer not connected to the ship's control network.

The following is a sample non-exhaustive list of cyber incidents, which should be addressed in plans for onboard contingencies. These incidents may be addressed in the company's procedures for dealing with shipboard emergencies as required by the ISM Code's Chapter 8 (Emergency preparedness).

- 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 of service incident.

Contingency plans and related information should include communications and escalation management to ensure that the correct shore based support can be accessed and should be available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

Contact details should be readily available for technical support from the operator's IT department or external IT contractors as appropriate.

*The ships security plan is confidential and approved by flag state. Where the master advises that the ship security plan and any other plans relating to security are confidential, the inspector should only confirm their existence by inspection of the front cover.*

*The inspector should address the question based on those documents and records that are not considered confidential in conjunction with the explanations of the accompanying officer.*

*Where a comment is required to support an observation, it must not provide any detail relating to the content of plans or risk assessments that are reported as confidential.*

## Suggested Inspector Actions

- Interview the officer with responsibility for cyber risk management on board to confirm the existence of
  - The company procedures for cyber risk management.
  - The inventory/register of sensitive IT/OT systems fitted on board.
  - Records of approval for external local or remote access to sensitive IT/OT systems.
  - Contact details for technical support from the operator's IT department or external IT contractors.
  - Records of cyber security training.
  - Cyber contingency plans in hard copy.

- During the tour of the vessel, inspect equipment to verify physical cyber security measures were in place.

## Expected Evidence

- Company procedures for cyber risk management.
- The inventory/register of sensitive IT/OT systems fitted onboard.
- Records of approval for external local or remote access to sensitive IT/OT systems.
- Cyber contingency plans in hard copy.
- Contact details for technical support from the operator's IT department or external IT contractors.
- Records of cyber security training.

*The inspector should not request to review any of the documents and records above considered to be confidential.*

## Potential Grounds for a Negative Observation

- There were no company procedures for cyber risk management that:
  - Identified the roles and responsibilities of users, key personnel, and management both ashore and on board.
  - Identified the IT and OT systems at risk on board.
  - Described technical protection measures to protect against a cyber incident.
  - Described procedural protection measures to protect against a cyber incident.
- The accompanying officer was not familiar with the company procedures for cyber risk management.
- A space containing sensitive IT or OT control equipment was not securely locked.
- There was no inventory/register of sensitive IT/OT systems fitted on board.
- Physical access to sensitive user equipment (such as exposed USB ports on bridge systems) was not secured or disabled.
- Company procedures did not designate who on board should have an administrator profile and/or who should manage user profiles.
- Back-up facilities were not available or not used.
- Officers were not familiar with the back-up arrangements for OT systems critical to navigation and propulsion.
- There was no evidence of formal approval for a technician observed on board to access sensitive equipment such as ECDIS etc.
- There was no evidence that portable media observed in use had been checked for malware etc. in a computer not connected to the ship's control network.
- It was reported that:
  - On-board computers were not protected by anti-virus software.

    - Anti-virus software had not been regularly updated.
    - Application software had not been regularly updated with upgrades and security patches.
    - A crew member other than a senior officer had an administrator profile.
    - User profiles allowed computer workstations to be used for other than their intended purpose.
    - User profiles were not actively managed.
    - Generic user profiles and passwords were passed on at crew changes.
- The accompanying officer had not received cyber security training as appropriate to their responsibilities and duties.
- User names and passwords were posted at workstations.
- It was observed that passwords were not required to access workstations.
- There was no evidence that cyber security awareness was actively promoted on board.
- There were no cyber contingency plans addressing the loss of:
    - Function or reliability of navigational equipment e.g., ECDIS.
    - Availability or integrity of external data sources such as GNSS.
    - Connectivity with the shore including GMDSS communications.
    - Control systems for critical systems such as propulsion, steering etc.
- There were no hard copies of cyber contingency plans.
- Contact details were not readily available for technical support from the operator's IT department or external IT contractors as appropriate.