Complying with the IMO 2021 Cybersecurity Regulations

Ensuring the safe and secured operation of vessels at sea and onshore

Background

The International Safety Management (ISM) code is an international standard for the management and operation of ships included in the International Convention for the Safety of Life at Sea (SOLAS). SOLAS is an international maritime treaty covering minimum safety standards for the equipment, construction, and operation of vessels. SOLAS covers over 150 nation-states, encompassing over 90% of merchant ships by gross tonnage.

On June 16, 2017, the International Maritime Organization (IMO) adopted Resolution MSC.428(98) that "encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021."

On July 5, 2017, the IMO issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. These guidelines provide "high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO."

Resolution MSC.428(98) and MSC-FAL.1/Circ.3 are included in the ISM Code (2018 Edition) as relevant appendices.

What is the objective? Per the IMO Guidelines on maritime cyber risk management, "the goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks."

What is required? The IMO resolution effectively addresses cyber risks as a part of safety management systems within the ISM Code. Nearly all of the international shipping community is required to comply with the ISM Code, as respective countries are parties to SOLAS. Therefore, to comply with the ISM Code, internationally voyaging vessels must address cyber risks within their safety management systems.

When is the deadline? The deadline for compliance is "before January 1, 2021 or the first annual verification of the company's DOC after January 1, 2021." To comply with the ISM Code, organizations will need to address their cyber risks at some during 2021 (if doing international business that year).

Who is affected? The ISM Code applies to the owner or anyone who assumes responsibility for the operation of the ship. Both owners and operators (if different) will need to comply.

Addressing cyber risks in compliance with the IMO/ISM 2021 cybersecurity regulations

Many industries and organizations address environment, health, and safety (EHS/HSE) and cyber risk management separately, often managed by entirely different departments. Conversely, IMO Resolution MSC.428(98) essentially merges the two seemingly separate 'disciplines' under one framework—risk management—encouraging maritime organizations "to ensure that cyber risks are appropriately addressed in safety management systems." There are considerable similarities between safety and cyber risk management practices, and the two clearly impact each other in today's digitally connected world. So, what does this look like?

First, the ISM code defines safety management systems (in which cyber risks should be addressed according to IMO Resolution MSC.428(98)) as:

> "Safety management system means a structured and documented system enabling company personnel to implement effectively the company safety and environmental protection policy."

Existing ISM code covers people, processes, and technology across elements such as incident response planning or emergency preparation. As such, addressing cyber risks within the safety management system—thereby in compliance with the IMO resolution and ISM Code—also touches on people, process, and technology covering all functional elements as further defined in the IMO guidelines. Addressing cyber risks should cover:

	Area of Focus		
Functional Elements	**People**	**Process**	**Technology**
Identify			
Protect			
Detect			
Respond			
Recover			

Importantly, the IMO recognizes "no two organizations in the shipping industry are the same" in its Guidelines on maritime cyber risk management. The IMO guidelines are expressed in "broad terms in order to have a widespread application." As such, they are not prescriptive in execution but fundamental principles and intent. Both the IMO guidelines and the ISM code require organizations to address cyber risks towards the aim of operational resiliency and across various elements within an organization.

While there is considerable room for interpretation, an approved safety management system must adequately address both the ISM code objectives (the intent) as well as functional elements (identify, protect, detect, respond, recover) in a manner that is concurrent and continuous in practice.

How to Begin

The following suggestions are based on correlating and merging the IMO resolution, IMO guidelines, ISM code, and industry guidelines referred to by the IMO. The resulting information is then organized in the following method to facilitate ease of understanding, identification of an organization's current cybersecurity posture, and the ability to identify gaps and implement safeguards at a high-level.

1. Assess Cyber Risks – Identify cyber risks to ships and operations
2. Design a Secure Cyber Architecture – Design a cyber risk management framework
3. Protect Vessels and Operations – Implement safeguards to ensure operational resiliency

Identifying cyber risks may not apply to organizations that may already know existing risks. In whichever method chosen for execution, establishing a cyber risk management framework, implementing appropriate safeguards, and updating the safety management system to reflect such adaptations are required to comply with IMO/ISM cybersecurity regulations.

The Partner You Can Trust

Our goal is singular: to help you prepare for and protect against cyber attacks.

Working with leading LNG, LPG, and oil tanker owners and operators as well as maritime industry bodies and standards groups, **Mission Secure** helps organizations secure their most critical assets and operations. Fortune 10 and Fortune 1000 clients across industries, including maritime, oil and gas, the U.S. military, smart cities, and critical infrastructure, rely on Mission Secure for the operational resiliency they require.

Contact Us Today to Learn More

www.MissionSecure.com

Info@MissionSecure.com · +1.832.925.8748

MSi
Mission Secure, Inc.

Mission Secure (MSi) is a leading industrial control system (ICS) cybersecurity company protecting clients in maritime, oil and gas, defense, and critical infrastructure from cyber attacks. The patented MSi Platform is the only end-to-end ICS cybersecurity solution with visibility and protection down to Levels 1 and 0.

Complying with the IMO 2021 Cybersecurity Regulations

Ensuring the safe and secured operation of vessels at sea and onshore

Assess Cyber Risks for Maritime

Recommended Actions

Comprehensively assess cyber risks across people, processes, and technology, including IT, OT, and data.

References | ISM Code: 1.2.2.2, 10.3; IMO Guide: 1.2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.9, 3.1, 3.4, 3.5.1; Industry Guide: 3, 4; ISO/IEC 27001: A.8.1.1, A.8.2.1, A.12.6.1, A.15.2.1, A.16.1.4, A.17.1.1-2

Reassess cyber risk implementation, review, reporting, and auditing functions of the safety management system.

References | ISM Code: 1.4.6, 2.2, 5.1.5, 10.2.1, 12.1; IMO Guide: 2.1.8, 3.3, 3.5, 3.6, 3.7; ISO/IEC 27001: A.5.1.2, A.9.1.1, A.9.2.5, A.12.6.1, A.12.7.1, A.13.2.4, A.14.2.3, A.15.2.2, A.16.1.4, A.17.1.3, A.18.2.1-3

Assess, Design, Protect.

Mission Secure can help secure your vessels and protect your operations.

Design a Secure Cyber Architecture

Recommended Actions

Design, establish, or incorporate cyber risk management into the organization's safety management system.

References | ISM Code: 1.2.2.2, 10.3; IMO Guide: 1.2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.9, 3.1, 3.4, 3.5.1; Industry Guide: 3, 4

A) One accepted IMO approach: Compare a current comprehensive cyber risk assessment to an organization's desired cyber risk management posture. This risk-based approach will enable an organization to apply its resources in the most effective manner.

Reference | IMO Guide: 3.4

B) Establish a cybersecurity policy or cyber risk management approach that covers:

- Achievement of objectives
- Five functional elements
- People, process, and technology

References | ISM Code: 1.2, 1.4, 2.1, 3.2, 3.3, 6.5, 7, 8.1, 8.2, 9.1, 9.2, 10.3, 10.4; IMO Guide: 1.5, 2.1.2, 2.1.8, 2.1.9, 3.1, 3.2, 3.3, 3.5; Industry Guide: 1, 3, 4, 5, 6, 7.1, 7.2, Annex 1; ISO/IEC 27001: A.5.1.1, A.6.1.1, A.6.2.1-2, A.7.1.1-2, A.7.2.1-3, A.7.3.1, A.8.1.3, A.8.2.1-3, A.9.1.1, A.9.2.1-2 & 4, A.9.3.1, A.10.1.1-2, A.11.1.1 & 3-5, A.11.2.9, A.12.1.1, A.12.2.1, A.12.3.1, A.12.6.1-2, A.12.7.1, A.13.2.1 & 4, A.14.2.1 & 5-6 & 9, A.15.`1.2, A.15.2.1-2, A.16.1.1 & 4 & 7, A.17.1.1-3, A.18.2.1-3

Update or adapt the safety management system to account for the cyber risk management framework (as designed above). Include relevant documentation.

References | ISM Code: 1.1.4, 1.2.2, 1.2.3.1, 1.4, 2.1, 3.2, 5.1, 6.5, 7, 8.1, 8.2, 9.1, 9.2, 10.3, 10.4; IMO Guide: 2.1.9, 3.5; Industry Guide: 1, 5.1; ISO/IEC 27001: A.5.1.1, A.6.1.1, A.6.2.1-2, A.7.1.1-2, A.7.2.1-3, A.7.3.1, A.8.1.3, A.8.2.1-3, A.9.1.1, A.9.2.1-2 & 4, A.9.3.1, A.10.1.1-2, A.11.1.1 & 3-5, A.11.2.9, A.12.1.1, A.12.2.1, A.12.3.1, A.12.6.1-2, A.12.7.1, A.13.2.1 & 4, A.14.2.1 & 5-6 & 9, A.15.`1.2, A.15.2.1-2, A.16.1.1 & 4 & 7, A.17.1.1-3, A.18.2.1-3

Protect Vessels and Operations

Recommended Actions

The functional elements—identify, protect, detect, respond, recover—should be incorporated in the risk management framework, concurrently and continuously. These functional elements encompass people, process, and technology.

References | ISM Code: 1.2.2, 1.2.3.1, 1.4; IMO Guide: 2.1.9, 3.5; Industry Guide: 1, 5.1; ISO/IEC 27001: A.6.2.2, A.7.3.1, A.8.1.1, A.8.2.1, A.8.3.3, A.10.1.1-2, A.11.1.1-2 & 4, A.11.2.1-4 & 8, A.12.2.1, A.12.3.1, A.12.4.2-3, A.13.1.1, A.13.2.1 & 3, A.14.1.2, A.14.2.6, A.14.3.1, A.16.1.4-6, A.17.1.1-3, A.18.1.3-4

Implement cyber risk management changes as outlined in the new or updated cyber risk management policy or framework. Include actions in or adapt the existing safety management system to account for cyber risk management.

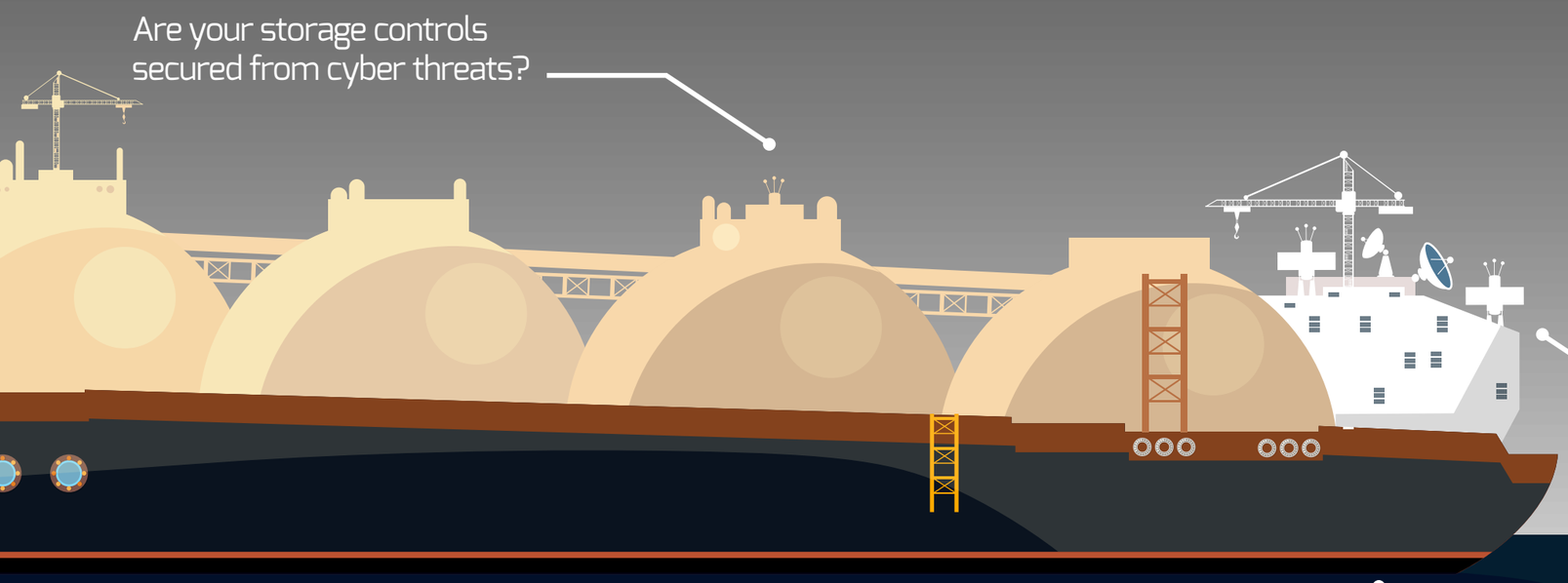
People: Roles, responsibilities, and resources (e.g., training).

Process: Policies, procedures, and accountability (e.g., reports and audits).

Technology: Systems, assets, and solutions. A cyber risk management framework should facilitate or enable the following, continuously and concurrently:

- Identification of critical assets (systems, data, etc.)
- Protection of critical assets
- Detection of cyber-events in a timely manner
- Responding to and recovering from a cyber-event

References | ISM Code: 1.2.2, 1.2.3.1, 1.4; IMO Guide: 2.1.9, 3.5; Industry Guide: 1, 5.1; ISO/IEC 27001: A.6.1.1-5, A.6.2.1-2, A.7.1.1-2, A.7.2.1-3, A.7.3.1, A.8.1.1-4, A.8.2.1-3, A.8.3.1-3, A.9.1.2, A.9.2.1-6, A.9.3.1, A.9.4.1-5, A.10.1.1-2, A.11.1.1-6, A.11.2.1-9, A.12.1.1-4, A.12.2.1, A.12.3.1, A.12.4.1-4, A.12.5.1, A.12.6.1-2, A.12.7.1, A.13.1.1-3, A.13.2.1-4, A.14.1.1-3, A.14.2.1-9, A.14.3.1, A.15.1.1-3, A.15.2.1-2, A.16.1.1-7, A.17.1.1-3, A.17.2.1, A.18.1.1-5, A.18.2.1-3



MSi
Mission Secure, Inc.

Disclaimer: Each organization under the ISM code should undertake an assessment of their existing safety management system in reference to the IMO resolution to address and safeguard against cyber risks, regardless of the manner in which that is accomplished.