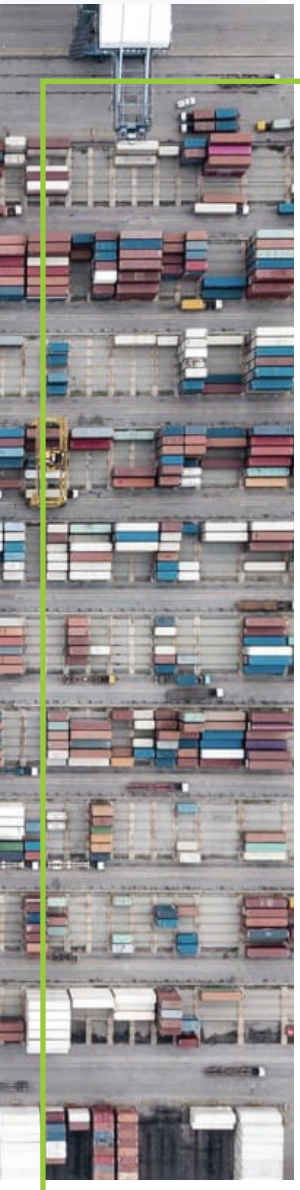
REGULATORY OVERVIEW

Mission Secure

Complying with the IMO 2021 Cybersecurity Regulations

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



Maritime cyber risk management to safeguard the operation of vessels at sea and onshore.

In recognition of the urgent cyber threats to global shipping, a significant cybersecurity compliance deadline facing the maritime industry is the International Maritime Organization's (IMO) Resolution MSC.428(98).

IMO Resolution MSC.428(98) "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."

IMO subsequently published guidelines to facilitate appropriate cyber risk management for vessel owners and operators. Based on the NIST cybersecurity framework and tailored for the maritime industry, these guidelines provide recommendations — including functional elements — to support effective cyber risk management. The IMO guidelines also reference additional guidance and standards, including:

- ✓ The *Guidelines on Cyber Security Onboard Ships* by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- ✓ ISO/IEC 27001 standard on information technology, security techniques, information security management systems, requirements, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The following overview correlates the key tenants of each document — IMO resolution, IMO guidelines (based on NIST), ISM Code, *Guidelines on Cyber Security Onboard Ships*, and ISO/IEC 27001. In this overview, the information presented is organized 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.

Assess Cyber Risks: Identify cyber risks to ships and operations

Design a Secure Cyber Architecture: Design a cyber risk management framework

Protect Vessels and Operations: Implement safeguards to ensure operational resiliency

Regardless of method, guide, or standard, 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 beginning January 1, 2021.

BACKGROUND

Safety and cybersecurity — hand-in-hand.

The International Convention for the Safety of Life at Sea (SOLAS) is an international maritime treaty establishing minimum safety standards for equipment, construction, and operation of merchant ships. SOLAS covers over 150 nation-states, encompassing more than 90% of merchant ships by gross tonnage.

SOLAS Chapter IX — *Management for the Safe Operation of Ships* — requires every shipowner and any person or company that assumes responsibility for a ship to comply with the International Safety Management Code (ISM).

The purpose of the ISM Code is to ensure safety at sea and prevent damage to property, personnel, and environment. In order to comply with the ISM Code, a company must be audited after submitting a Safety Management System Manual (SMS), approved by a Flag Administration or Recognized Organization.

Upon successful audit, the following certifications are issued:

- ✓ Document of Compliance (DOC) — issued to the company
- ✓ Safety Management Certificate (SMC) — issued to each vessel

NEW CYBERSECURITY REGULATIONS

Addressing cyber risk management

To address increasing cyber threats to maritime operations and mitigate new cyber risks, the following were adopted by the IMO and added to the ISM Code (2018 Edition).

- **Resolution MSC.428(98):** On June 16, 2017, the 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."

- **MSC-FAL.1/Circ.3:** 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."

> *...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."*
>
> IMO Resolution MSC-FAL.1/Circ.3

What is the objective?

Per the IMO *Guidelines on maritime cyber risk management*, the goal of Resolution MSC.428(98) 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, in order 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." In order to be in compliance with the ISM Code, organizations will need to address their cyber risks at some point 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 be in compliance.

Importantly, port operations play an equally critical role in the maritime industry. While port operations do not fall under Resolution MSC.428(98), it is pertinent that port facilities undertake appropriate cybersecurity measures — to protect both themselves as well as clients coming to and relying on the safe and secure operation of port facilities. Moreover, as vessels bolster their cybersecurity postures, owners and operators may show reluctance in working with port facilities that do not share their level of cyber risk management as port cyber incidents have the potential to impact vessels and at sea operations.

Complying 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 — operational 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 (to include cyber risks) as:

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

FUNCTIONAL ELEMENTS OF CYBER RISK MANAGEMENT

The existing ISM Code covers people, process and technology across elements such as incident response planning or emergency situation 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:

- ✓ **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.
- ✓ **Protect:** Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- ✓ **Detect:** Develop and implement activities necessary to detect a cyber-event in a timely manner.
- ✓ **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.
- ✓ **Recover:** Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

SCOPE

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 in 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.

ACHIEVING COMPLIANCE

How to begin

The following sections correlate the key tenants of each document provided or referenced by the IMO, including the IMO resolution, the IMO guidelines (based on NIST), the ISM Code, the *Guidelines on Cyber Security Onboard Ships* (published by BIMCO, et al.), and the ISO/IEC 27001 standard. The information is organized 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. The following sections include:

Assess Cyber Risks: Identify cyber risks to ships and operations

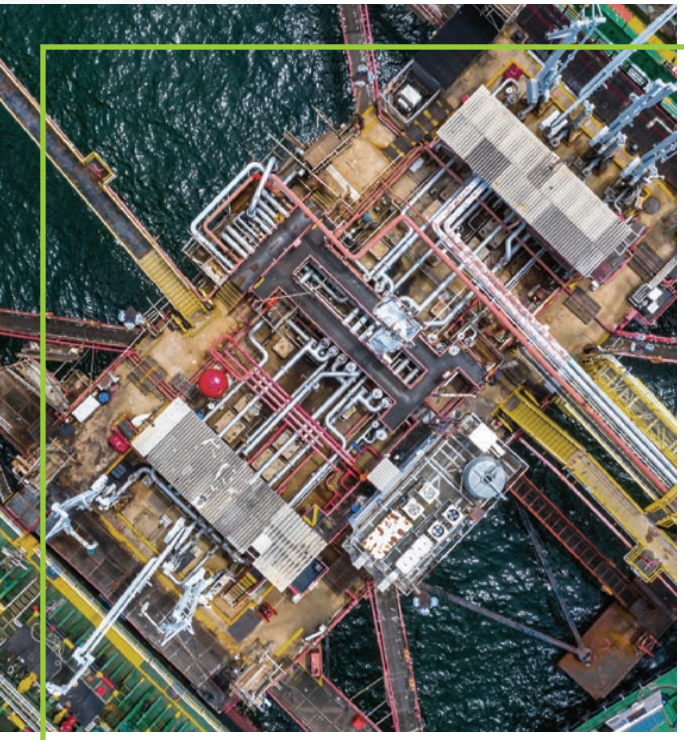
Design a Secure Cyber Architecture: Design a cyber risk management framework

Protect Vessels and Operations: Implement safeguards to ensure operational resiliency

To further assist organizations as they prepare for compliance and track their progress, a high-level checklist is also provided at the end this overview.

What’s covered

- ✓ IMO Resolution MSC.428(98)
- ✓ MSC-FAL.1/Circ.3 *Guidelines on maritime cyber risk management*
- ✓ The *Guidelines on Cyber Security Onboard Ships* by BIMCO, et al.
- ✓ ISO/IEC 27001
- ✓ U.S. NIST Framework for Improving Critical Infrastructure Cybersecurity



Assess cyber risks

Cyber-related risk and threats to your vessel and operational networks are mounting, and so are the maritime industry cybersecurity compliance requirements. Between the IMO Resolution MSC.428(98) and other programs like the Tanker Management and Self Assessment (TMSA), you'll need to get a handle on your vessel IT and operational technology (OT) networks before you can even commence.

Cyber risk assessments can help jump-start your efforts to create a cybersecurity strategy and establish an initial baseline of cybersecurity requirements and internal standards for your vessel networks. For that reason, the majority of cybersecurity frameworks and regulations have an assessment component — IMO included.

> *In the context of a ship's operation, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company* ***needs to assess risks arising from the use of IT and OT onboard ships*** *and establish appropriate safeguards against cyber incidents."*
>
> Guidelines on Cyber Security Onboard Ships
>
> BIMCO, et al.

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 Cyber Risks for Maritime: Recommended Actions

Cyber Risk Assessments

Comprehensively assess cyber risks across people, processes, and technology, including IT, OT, and data.
Reassess cyber risk implementation, review, reporting, and auditing functions of the safety management system.

CYBER RISK ASSESSMENTS

People

Comprehensively assess cyber risks including, but not limited to:

- ✓ Cyber discipline or cyber hygiene lapses
- ✓ Management, operational, or procedural controls
- ✓ Design, operation, integration, or maintenance inadequacies
- ✓ Inappropriate or procedural lapses by operational personnel or third parties

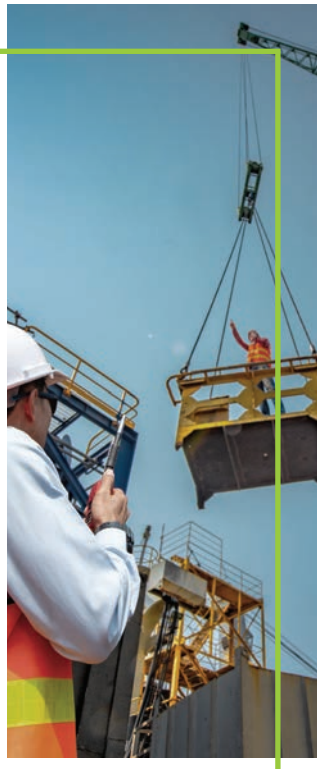
CYBER RISK ASSESSMENTS

Process

Comprehensively assess cyber risks including, but not limited to:

- ✓ Threats from benign, malicious, intentional, unintentional, current, or emerging sources
- ✓ Impacts to safety and security
- ✓ Management, operational, or procedural controls
- ✓ Design, operation, integration, or maintenance inadequacies
- ✓ Inappropriate or procedural lapses by operational personnel or third parties

> *The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks."*
>
> IMO MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management



CYBER RISK ASSESSMENTS

Technology

Comprehensively assess cyber risks including, but not limited to:

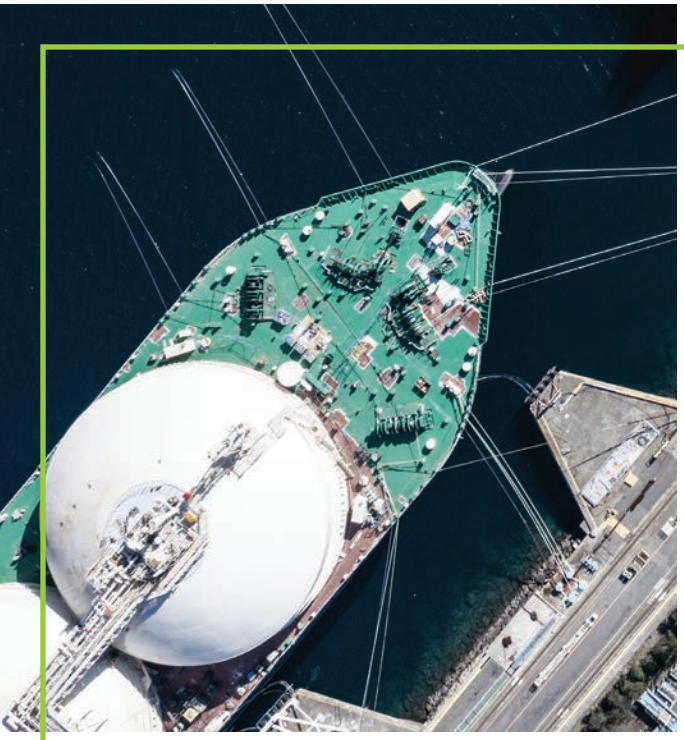
- ✓ Information technology (IT) and operational technology (OT) equipment and systems
- ✓ Information and data exchanged within systems
- ✓ Design, operation, integration, or maintenance inadequacies
- ✓ Operational and technical controls
- ✓ Critical assets, including equipment, technical systems, or data where their sudden operational failure may result in hazardous situations
- ✓ Vulnerable systems could include, but are not limited to:
    - ✓ Bridge systems;
    - ✓ Cargo handling and management systems;
    - ✓ Propulsion and machinery management and power control systems;
    - ✓ Access control systems;
    - ✓ Passenger servicing and management systems;
    - ✓ Passenger-facing public networks;
    - ✓ Administrative and crew welfare systems; and
    - ✓ Communication systems.

CYBER RISK ASSESSMENTS

Reassessments

Incorporate cyber risk management into the implementation, review, reporting, and auditing functions of the safety management system, including:

- ✓ Ensure policy implementation at all levels of the organization, onboard and ashore
- ✓ Periodically review and report deficiencies
- ✓ Hold inspections at appropriate intervals
- ✓ Carry out internal safety audits, onboard and ashore, encompassing cyber risk management as it impacts safety
- ✓ Establish or extend the safety management system to constitute an ongoing process of feedback mechanisms in relation to cyber risk management



Design and document a secure cyber architecture

Organizations in the maritime industry will have different needs and levels of maturity when it comes to the breadth of their vessel IT and OT networks and cyber-related systems, so approaches to securing their maritime cyber architectures will vary. A couple of methods are described for maritime organizations to design a secure maritime cyber architecture; both are covered in the following section as you design your secure cyber architecture.

Organizations must also update their safety management system, including relevant documentation, to account for their maritime cyber risk management framework.

> *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****."*
>
> Guidelines on maritime cyber-risk management
>
> IMO

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

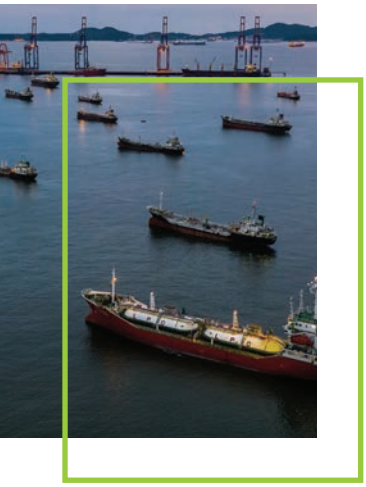
Update or adapt the safety management system to account for cyber risk management framework. Include relevant documentation.

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

Design a Secure Cyber Architecture: Recommended Actions

Cyber Risk Management in the Safety Management System

Design, establish, or incorporate cyber risk management into the organization's safety management system. Update or adapt the safety management system to account for cyber risk management framework (as designed above). Include relevant documentation.



DESIGN A SECURE CYBER ARCHITECTURE

Option A

One accepted IMO approach (if applicable): 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 best apply its resources in the most effective manner.

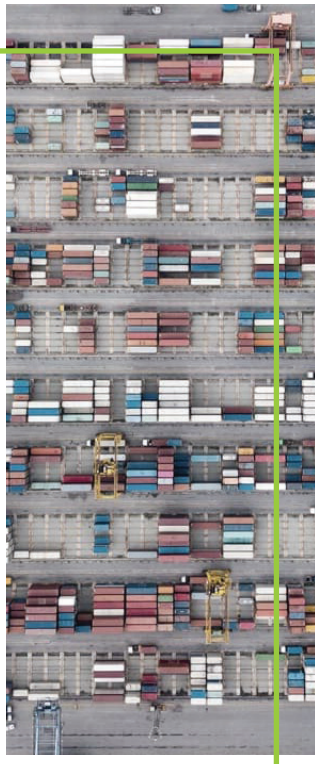
- ✓ Identified gaps can be addressed to achieve risk management objectives through a prioritized cyber risk management plan

DESIGN A SECURE CYBER ARCHITECTURE

Option B

Establish a cybersecurity policy or cyber risk management approach encompassing the elements below:

- ✓ Achievement of the following objectives:
  - ✓ Cybersecure practices in ship operation and working environment
  - ✓ Assessment of all identified cyber risks to ships, personnel, and environment
  - ✓ Continuous improvement of cyber risk management skills, including emergency preparation
- ✓ Achievement of the following functional elements:
  - ✓ **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.
    - ✓ Reference the risk posed by unmitigated cyber risks



- ✓ Identification of OT and IT systems the sudden operational failure of which may result in hazardous situations
- ✓ Identification of potential emergency shipboard situations
- ✓ Engagement of senior management support
- ✓ Define roles and responsibilities of personnel for cyber risk management
- ✓ Identification of any cyber training required
- ✓ Identification of any required resources or support

✓ **Protect:** Develop risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

- ✓ Implementation of risk control measures
- ✓ Establish appropriate safeguards
- ✓ Define cyber risk procedures, plans, and instructions
- ✓ Define emergency plans to include responses to cyber incidents

✓ **Detect:** Develop activities necessary to detect a cyber-event in a timely manner.

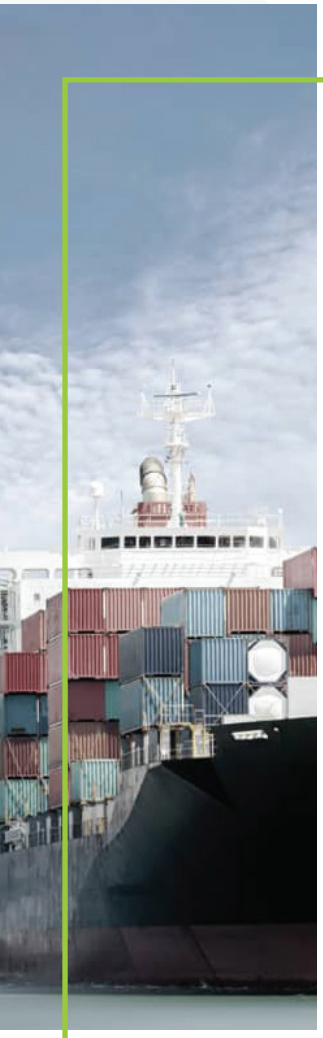
- ✓ Develop capabilities or activities necessary to detect a cyber-event in a timely manner
- ✓ Define procedures for reporting non-conformities, accidents, and hazardous situations relating to cyber incidents

✓ **Respond:** Develop activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

- ✓ Develop activities and plans to provide resilience
- ✓ Develop activities and plans to provide systems necessary for shipping operations or services impaired by a cyber-event
- ✓ Develop procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence
- ✓ Include specific measures aimed at promoting the reliability of OT

✓ **Recover:** Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

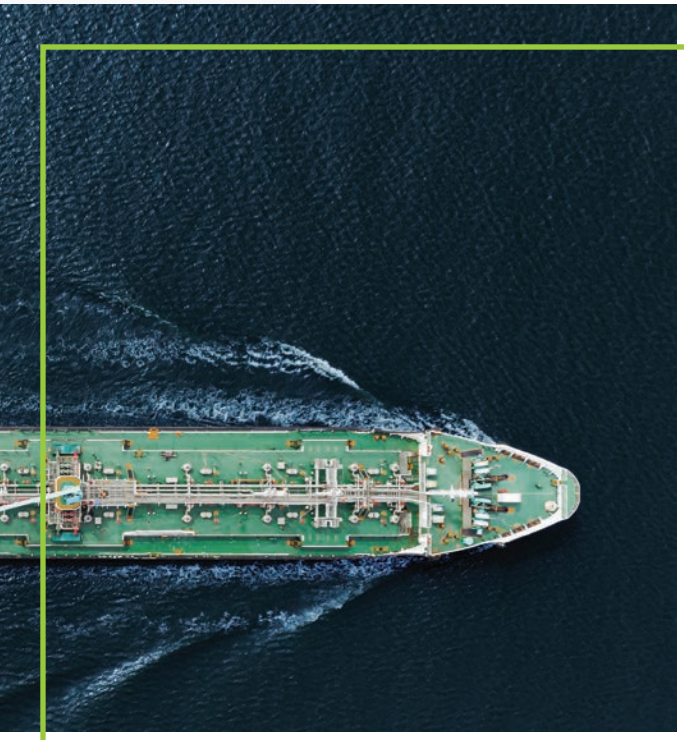
- ✓ Develop measures to back-up and restore cyber systems
- ✓ Creation and maintenance of back-ups into the ship's operational maintenance routine
- ✓ Establish regular testing of stand-by arrangements not in continuous use
- ✓ Incorporate cyber-related emergency drills and exercises



Updating the Safety Management System for Cyber Risks

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

- ✓ Document how cyber risk management objectives will be achieved or adapt existing language
- ✓ Document roles and responsibilities of personnel for cyber risk management
- ✓ Document procedure for ensuring and maintaining resources for cyber risk management
- ✓ Document cyber risk procedures, plans, and instructions
- ✓ Document cyber risk emergency and incident response plans
- ✓ Document procedures for cyber non-conformity, accident, or incident reporting
- ✓ Document procedures for corrective actions and recurrence prevention
- ✓ Document identified critical assets where the sudden operational failure could create hazardous situations
- ✓ Document specific measures aimed at promoting reliability and resiliency
- ✓ Document procedures for the creation and maintenance of back-ups within the ship's operational maintenance routine



Protect vessels and safeguard operations

Ultimately, the goal of the IMO Resolution is to protect vessels and maritime operations.

Now is the time to review your operations and management of your vessels to ensure their security, safety, and reliability from the onslaught of emerging cyber-attacks. With a thorough and effective cybersecurity risk management approach, you'll be able to ensure that you have the resources needed to protect your onshore and offshore operations. And with real-time visualization of your data and protection of critical assets and continuous monitoring across your vessels and maritime operations, you will be on your way to achieving IMO cybersecurity compliance.

> *Stakeholders should take the necessary steps to* **safeguard shipping from current and emerging threats** *and vulnerabilities related to digitization, integration and automation of processes and systems in shipping... Risk management is fundamental to safe and secure shipping operations.*
>
> Guidelines on maritime cyber-risk management
>
> IMO

The functional elements should be incorporated in the risk management framework, concurrently and continuously. Include actions in the existing SMS to account for cyber risk management.

References | ISM Code: 1.2.2, 1.2.3.1, 1.4; IMO Guide: 2.1.9, 3.5; Industry Guide: 1, 5.1

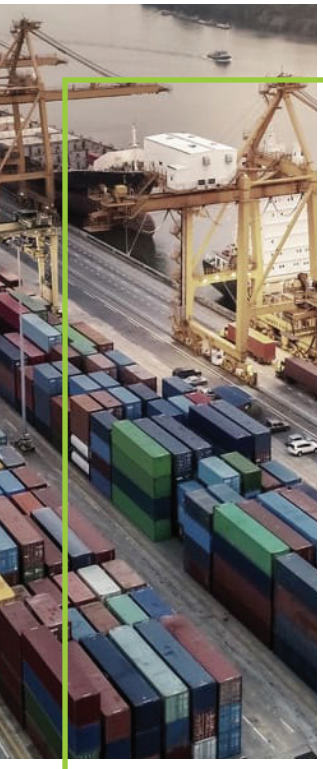
Implement cyber risk management changes as outlined in the new or updated cyber risk management policy or framework.

References | ISM Code: 1.2.2, 1.2.3.1, 1.4; IMO Guide: 2.1.9, 3.5; Industry Guide: 1, 5.1

Protect Vessels and Operations: Recommended Actions

Establishing Concurrent and Continuous Cyber Risk Management

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



PROTECT VESSELS AND OPERATIONS

Implement safeguards to ensure operational resiliency

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.

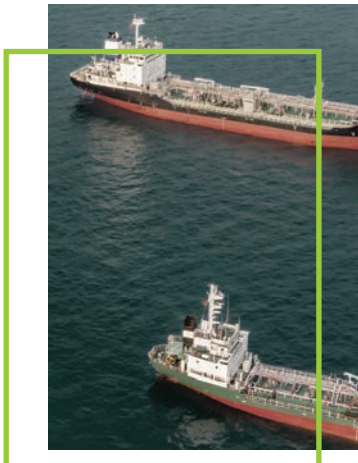
- ✓ **People:** Roles, responsibilities, and resources (e.g., training).
- ✓ **Process:** Policies, procedures, and accountability (e.g., reports and audits).
- ✓ **Technology:** Systems, assets, and solutions. A cyber risk management framework should facilitate or enable the following, continuously 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

PROTECT VESSELS AND OPERATIONS

Implementation across technology

The following examples are for illustrative purposes and not specifically addressed in the ISM Code.

- ✓ **Cyber Risk Management:** The following examples could be incorporated in a cyber risk management dashboard or console.
    - ✓ Monitor the cyber risks to the operation of each vessel
    - ✓ Visualize data and manage the security of critical assets



- ✓ Ensure adequate resources and shore-based support are applied
- ✓ Manage workflows, rules, users, third-party access, and corrective actions
- ✓ Familiarization of duties and instructions

✓ **Identification of Critical Cyber Assets (systems, data, etc.):** The following examples could be incorporated into ongoing identification of critical assets.

- ✓ Identify all connected devices and communications
- ✓ IT and OT network traffic monitoring
- ✓ Inventory and manage IT and OT assets
- ✓ Inventory and monitor OT communications and protocols
- ✓ Device hardening and patching

✓ **Protection of Critical Cyber Assets:** The following examples could be incorporated into ongoing risk control methods and contingency planning.

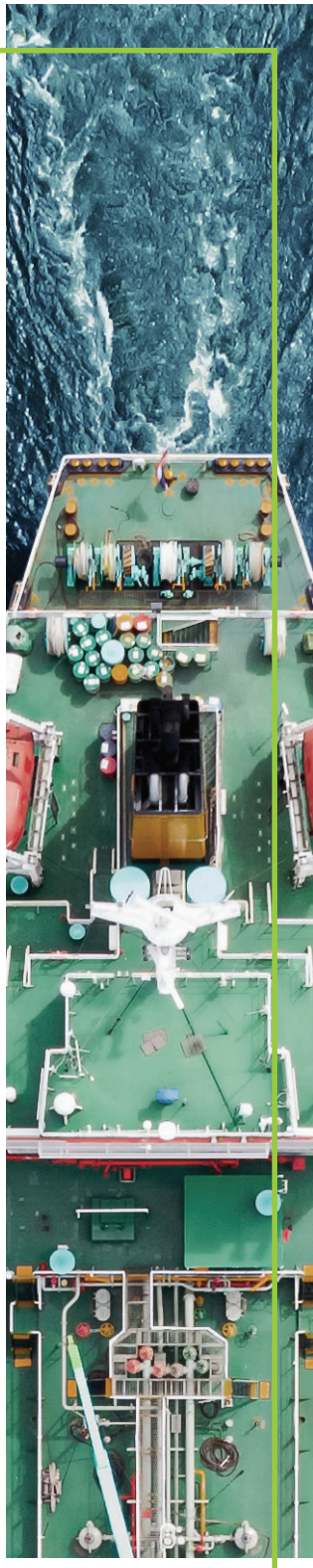
- ✓ Create logical security zones, segmentation, or micro-segmentation
- ✓ Limit communications by device and protocol
- ✓ Monitor external communications and prevent unauthorized access
- ✓ Managed all external communications and block unknown activity
- ✓ Critical device protections, including controllers, PLCs, safety systems, etc.

✓ **Detection of Cyber-events in a Timely Manner:** The following examples could be incorporated into ongoing cyber-event detection.

- ✓ Threat monitoring and breach detection
- ✓ Abnormal event or change detection
- ✓ Monitor raw electrical signals from critical processes
- ✓ Validate signal integrity from process to workstation or against set point
- ✓ Detect process cyber threats before damage occurs

✓ **Respond to and recovering from a cyber-event:** The following examples could be incorporated into ongoing cyber-event response and recovery planning.

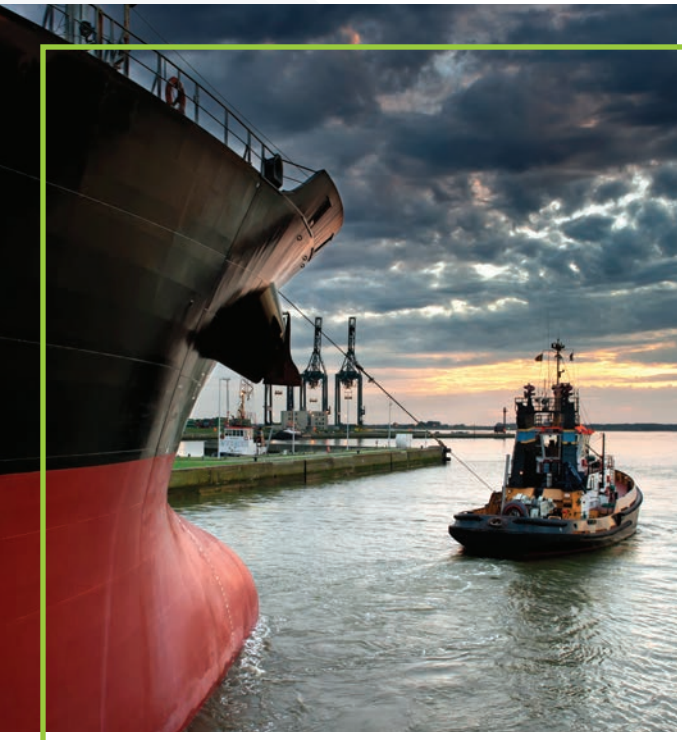
- ✓ Leverage a security operations center and SIEM for managing real-time alerts
- ✓ Develop a security incident response, investigation, and response capabilities



IMO 2021 Cybersecurity Regulations

Your High-level Category Checklist

ASSESS CYBER RISKS FOR MARITIME		DESIGN A SECURE CYBER ARCHITECTURE		PROTECT VESSELS AND OPERATIONS	
✓	**Recommended Actions**	✓	**Recommended Actions**	✓	**Recommended Actions**
	Comprehensively assess cyber risks across people, processes and technology, including IT, operational technology (OT) and data.		Design, establish or incorporate cyber risk management into the safety management system.		Incorporate the functional elements in the risk management framework, concurrently and continuously.
	Reassess cyber risk implementation, review, reporting and auditing functions of the safety management system.		**A)** Compare a current comprehensive cyber risk assessment to an organization's desired cyber risk management posture.		Include actions in the safety management system.
					Implement cyber risk management changes, including:
			B) Establish a cybersecurity policy or management approach that covers: • Achievement of objectives • Five functional elements • People, process and technology		**People** (Responsibilities, roles, etc.)
					Process (Procedures, policies, etc.)
					Technology (Systems, assets, etc.)
					Identify critical assets
					Protect critical assets
			Update or adapt the safety management system to account for cyber risk management framework (as designed above). Include relevant documentation.		Detect cyber-events
					Responding to and recovering from a cyber-event



> *Safety and cybersecurity are not based on frameworks or checklists; for us, it is a habitual action. We have lower downtime than our competitors due to the preventative maintenance we implement on our vessels. Cybersecurity is a key program in minimizing downtime risk as well. We are extremely pleased with our partnership with Mission Secure to improve our overall operational cybersecurity."*
>
> Vice President of IT
>
> LNG Global Shipping Provider

ADDITIONAL RESOURCES

Is your safety management system audit-ready?

Readiness begins with understanding your current cybersecurity posture. A trusted partner can help.

Mission Secure is offering a limited-time, **complimentary IMO 2021 Cyber Readiness Review**. The Readiness Review is a simple, no-cost, three-step process for establishing your organization's cyber readiness baseline.

- **Cyber Overview:** Mission Secure provides a 30-minute primer on IMO 2021 compliance and maritime sector-specific considerations. Obtain answers to compliance questions and secure your cybersecurity bearings.
- **Cyber Readiness Screener:** Participate in a guided, 60-minute cybersecurity self-assessment drawing upon the most common frameworks used in the maritime sector today.
- **Scorecard and Recommendations:** Receive a complimentary IMO Readiness scorecard with recommendations for further action. Understand your organization's alignment with the major cybersecurity frameworks and begin charting a course for increased security.

We're Here to Help

OT solutions backed by industry experts so you can trust your operations are properly regulated and locked down against cybersecurity threats.

LEARN MORE

Mission Secure

Mission Secure

Stop OT Cyber Threats Head-On

Mission Secure is setting a new standard in OT cyber-protection stopping OT cyber threats head-on. The Mission Secure Platform backed by 24/7 Managed Services is the first to seamlessly integrate OT visibility, segmentation, protection, threat hunting, and incident response, delivering military strength, industrial grade OT protection. With Mission Secure, defense, critical infrastructure, and process industry customers keep critical operations up and running and safe from harm.