CYBER SECURITY AT SEA

MARITIME CYBER SECURITY & RISK MANAGEMENT:

QUICK GUIDE TO IMO, ISO/IEC 21005, CIA TRIAD & NIST RECOMMENDATIONS

DRYAD ® GLOBAL

Introduction

Most vessel and shore-side networks are **not secure**.

State and non-state actors are perpetrating attacks on vessels, their owners, crew, operators and management companies daily.

Cyber experts are reporting a marked increase in direct cyber attacks to the maritime industry and maritime assets including vessels. In the Asia-Pacific region alone, cyber attacks targeting the maritime sector increased 168% in 2021.*

Effective **1 January 2021**, cyber security plans are a formal requirement for every SOLAS class vessel's **International Safety Management (ISM) Plan** - as mandated by the **International Maritime Organization (IMO)**.

> *Organised attackers who wish to cause* ***maximal disruption*** *are increasingly looking at maritime ports and vessels as primary targets for their attacks.*
>
> *- Dr Kemedi Moara-Nkwe*
> *University of Plymouth Research Fellow, Maritime Cyber Threats*

Dryad Global, through our **ARMS Cyber** platform, provides a variety of services to help you identify, protect, detect, respond and recover from cyber attacks. We provide specific regulatory language for your ISM plan and have a 100% track record of IMO vessel compliance success.

**Source: 'Beyond Compliance – Cyber Risk Management After IMO 2021' Thetius Report via inmarsat.com/maritime/2022/beyond-compliance-cyber-report.html*

IMO's **MSC-FAL.1/Circ.3** involves guidelines for maritime cyber risk management.

These guidelines provide high-level recommendations on maritime cyber risk management to safeguard against **current and emerging cyber threats and vulnerabilities**. They also include functional elements that work to support effective cyber risk management.

> "VULNERABILITIES CREATED BY ACCESSING, INTERCONNECTING OR NETWORKING SYSTEMS CAN LEAD TO CYBER RISKS WHICH SHOULD BE ADDRESSED." *- IMO: MSC-FAL.1/CIRC.3*

MSC-FAL.1/Circ.3 **lists the following systems as often open to vulnerabilities:**

- BRIDGE SYSTEMS
- ACCESS CONTROL SYSTEMS
- CARGO HANDLING & MANAGEMENT SYSTEMS
- PASSENGER SERVICING AND MANAGEMENT SYSTEMS
- PROPULSION AND MACHINERY MANAGEMENT AND POWER CONTROL SYSTEMS
- PASSENGER FACING PUBLIC NETWORKS
- ADMINISTRATIVE AND CREW WELFARE SYSTEMS
- COMMUNICATION SYSTEMS

The IMO's cyber security recommendations can be incorporated into your existing risk management processes and are complementary to the other safety and security management practices already established by IMO.

ISO/IEC 27005

ISO 27005 (also called ISO/IEC 27005) is the latest standard set by the **International Organisation for Standardisation** and **International Electrotechnical Commission**'s 'ISO/IEC 27000 series.' This series acts as a cyber-risk toolkit, helping people with information security management systems to keep up with global IT security techniques and requirements.

ISO certification is not obligatory, but it is the industry standard recommended by the International Maritime Organisation. The IMO promotes ISO/IEC 27001 (the flagship ISO standard for cyber security) and its series of updates as "best practices for the implementation of cyber risk management."

WHY CONSIDER ISO 27005?

- ISO/IEC 27005 provides the practical keys for how you will be able to manage your information security risks effectively in compliance with ISO/IEC 27001.
- Compliance with ISO/IEC 27001 through ISO 27005 will also demonstrate that you have a cutting-edge and robust system of risk processes in place, building the confidence of your customers, passengers, and/or stakeholders.

SINCE 2020, MORE THAN **84,000** UNIQUE LOCATIONS (SITES) HAVE EARNED ISO 27001 CERTIFICATION.

Dryad Global looks at ISO 27005 in the context of maritime cyber security and risk mitigation to offer specific compliance support to ensure your crew & captains have an ISM plan to minimise risk from attack vectors.

CIA TRIAD

The CIA Triad is one effective framework for assessing the vulnerability of a ship's systems OR the impact of a cyber threat/ cyber attack. **'CIA' stands for each piller of the framework: confidentiality, integrity, and availability.**

CONFIDENTIALITY

Is there a loss of information confidentiality?

This could involve:

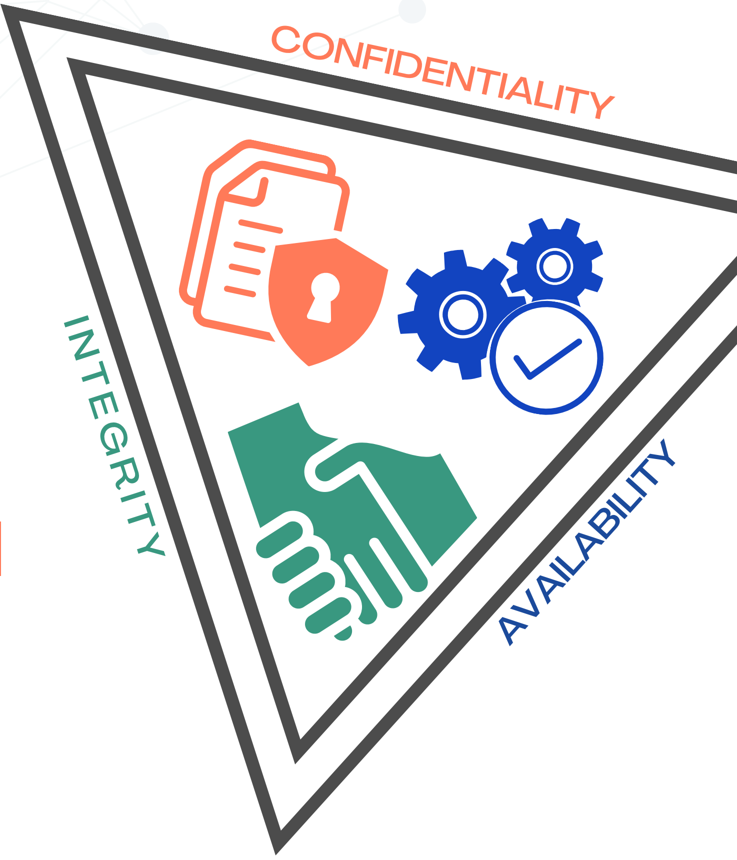
- unauthorised access to a vessel's data regarding crew, cargo, or passengers.
- disclosure of confidential information regarding the vessel, its crew, cargo, or passengers.

INTEGRITY

Is there a loss of data integrity?

This could involve:

- modification of information/data regarding the vessel and its management.
- danger to the operation and efficiency of the vessel's systems.



AVAILABILITY

Is there a loss of availability?

This could involve:

- destruction of information/data.
- disruption to the operation of the vessel's systems.

The relative importance of each pillar varies based on how the data is used.

Generally, confidentiality concerns relate to a vessel's information technology while integrity and availability relate more to its operational technology. The **CIA framework** is effective for assessing the security of **both the IT and OT** of a vessel's critical systems.