The ISM Code, supported by the IMO Resolution MSC.428 (98), requires ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system, until the first Document of Compliance after 1 January 2021.

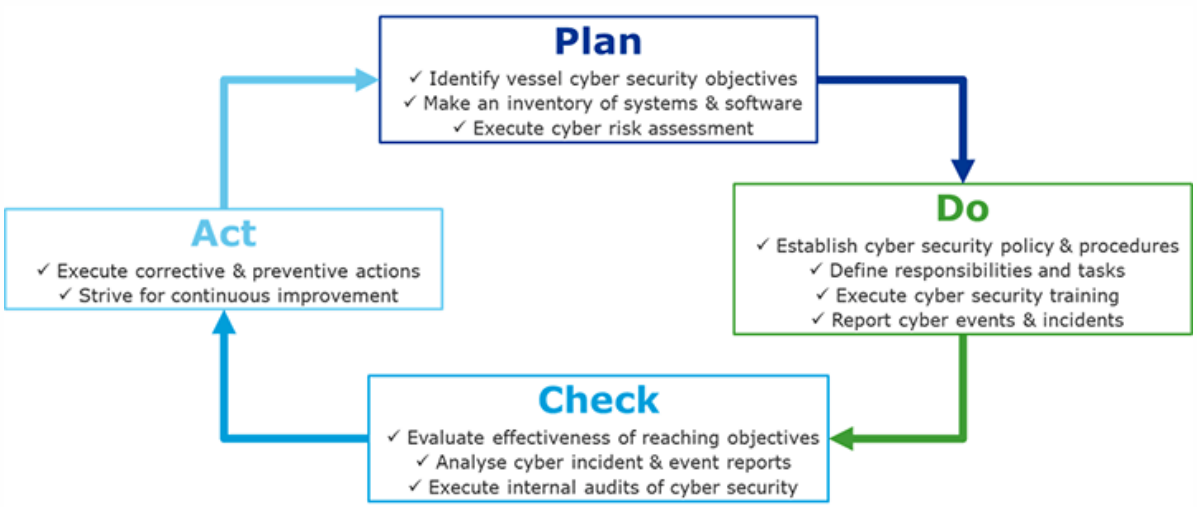
In combination with the resolution, the IMO also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) in July 2017. As both leave much of the interpretation to the company responsible for the safety management system, there are still many uncertainties of how to handle the requirements.

Below follow some concrete suggestions on how to ensure compliance with the IMO requirements and recommendations.

Recommended steps to ensure IMO`s Cyber Security compliance

The IMO agreed that cyber risk management should be integrated into existing management systems under the ISM Code and ISPS Code.

Accordingly, the following PDCA process should be applied:

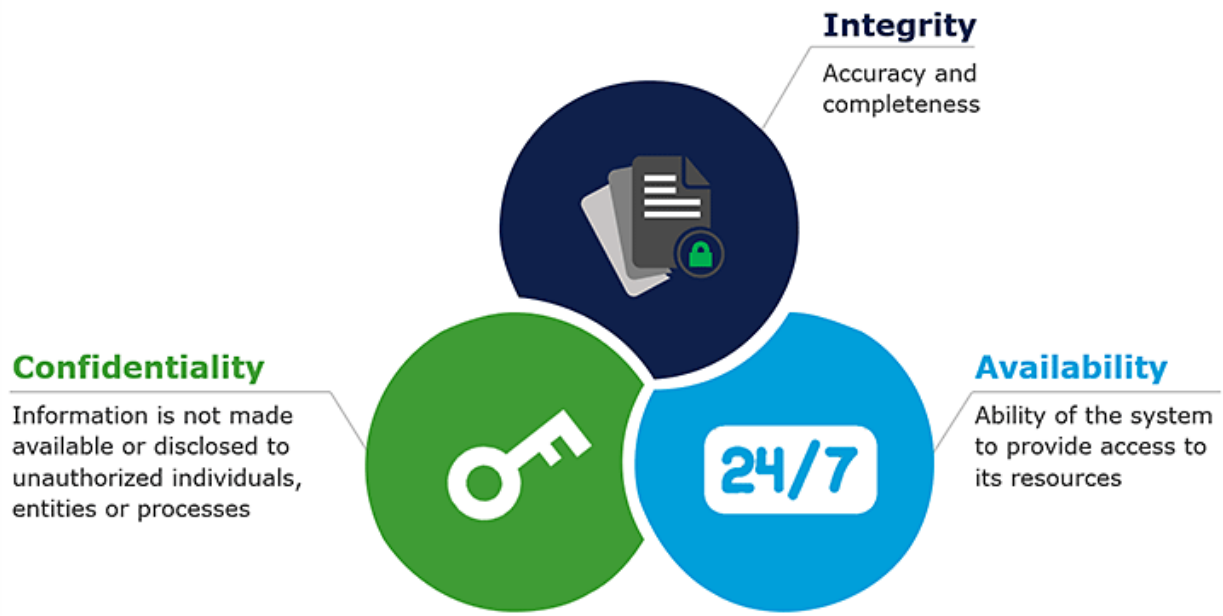


Plan

The first step is to identify cyber security objectives relevant for the safe operation of the vessel. In addition to the IMO requirements, other internal and external stakeholder requirements on cyber security should be accounted for when determining the objectives. Pursuant to the defined objectives, an inventory list of all safety and business-critical systems and software should be generated. The inventory, as well as network drawings showing the system connectivity, are prerequisites for executing a cyber-risk assessment. The assessment should include:

- Consequence analysis in terms of loss of confidentiality, integrity and availability of each system
- Likelihood analysis to determine how often the specific system is expected to be compromised
- Ranking of the asset according to its cyber security risks
- Determination of required barriers in terms of people, processes and technology improvements (for suggestions of barriers, see DNV GL's Cyber secure class notation)

For more detailed information on how to execute cyber risk assessments for vessels and offshore assets, see DNVGL-RP-0496.



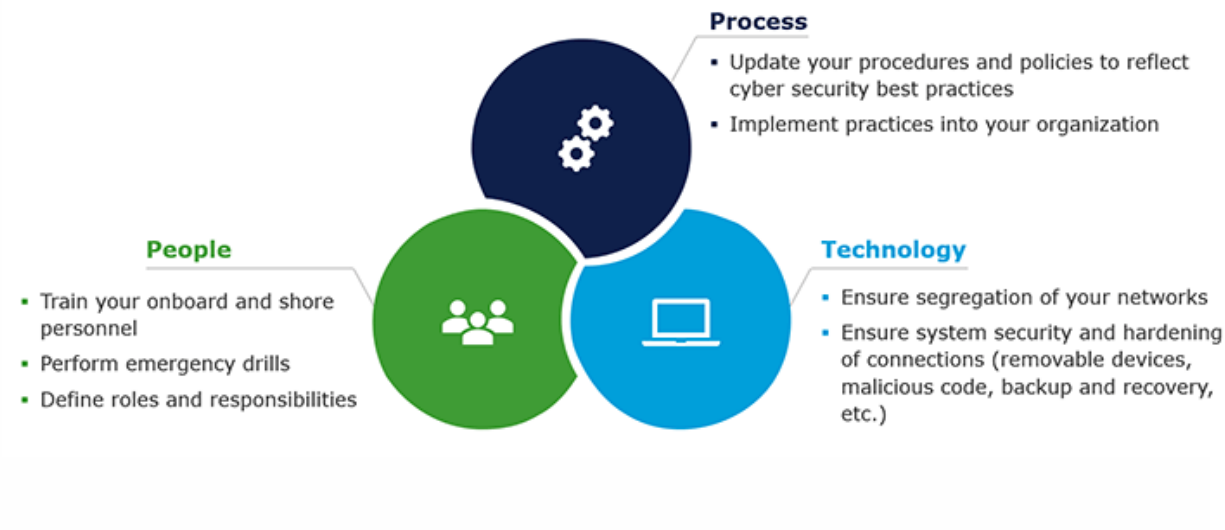
Do

The cyber risk assessment results should be utilized to define an implementation plan for rolling out suitable barriers.

Furthermore, as a minimum, the following functional requirements for the Safety Management System are applicable:

- A cyber security policy
- Instructions and procedures to ensure cyber-secure operation
- Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel concerning cyber security
- Procedures for reporting cyber-attacks, incidents and non-conformities
- Procedures to prepare for and respond to cyber-attacks and incidents
- Procedures for internal cyber security audits and management reviews

DNV GL recommends executing different levels of training, including general awareness for all crew and personnel, as well as trainings for specific system users, on-board cyber security officers and internal auditors.



Check

The effectiveness of the cyber security measures must be checked on a continuous basis. Internal checks include:

- Evaluation of effectiveness of achieving cyber security objectives
- Analysis of cyber incident and event reports
- Evaluation of logs and intrusion detection systems
- Execution of internal audits of cyber security
- Execution of cyber security incident response drills

Furthermore, external checks are recommended in order to ensure

- increased cyber security resilience,
- improved customer and business partner confidence, and
- compliance with IMO requirements.

Act

Based on the findings of the internal and external review reports, corrective and preventive actions should be implemented.

As the vessels and systems are increasingly interconnected and malicious cyber threats are continually changing, key to future successful cyber security resilience is to continuously improve by updating the cyber risk assessment, policies and procedures.

DNV GL Cyber Secure Class Notation as framework for IMO compliance

Our Cyber Secure class notation covers the IMO requirements and provides a framework of continuous external verification of effective cyber security through audits and penetration testing.