MARITIME

CYBER SECURITY SERVICES AND SOLUTIONS

Improve your cyber security with tailored solutions

Tailored solutions for systems, software and procedures as well as staff and crew to help you improve your cyber security resilience and protect your assets against the increasing threat to cyber physical systems and software.

Coping with cyber challenges and regulations
Recent years have shown rapid growth in the reach and complexity of cyber attacks in the maritime industry, often resulting in loss of critical operational technology (OT) systems. To account for the new threats, regulations and laws are being introduced that oblige owners, operators and managers to consider cyber risks, such as the IMO Resolution MSC.428(98). It requires stakeholders to include cyber risk management into their safety management system.

Furthermore, commercial cyber requirements and risks, like TMSA 3 for tankers and lack of insurance coverage in case of a cyber incident, can impact the probability of getting a charter and may lead to significant financial risk. New technology, more automation and digitalization that enable our industry to be more efficient also often come along with new cyber risks.

As a consequence, cyber security has become a concern and should be considered as an integral part of overall safety management in shipping and offshore operations.

The answer: holistic approach to multifaceted problem
With multifaceted vulnerabilities and cyber-attack scenarios, the answer lies in a holistic approach to reducing the risks of cyber attacks and in a response mechanism for mitigating consequences in the event that defences are successfully breached. DNV GL uses a systematic and holistic approach to assess the cyber security of vessels and their interaction with land-based management. Best practices from risk management in maritime, oil and gas, and energy applications come together to identify threats and build counterstrategies, looking at technical, procedural and behavioural aspects.

Proven cyber security management approaches include:
- Raising awareness of all stakeholders, including onshore personnel and offshore crews
- Assessing and implementing defensive and reactive countermeasures in terms of people, processes and technology
- Monitoring and reviewing the effectiveness and robustness of barriers, emphasizing continuous improvement
Our approaches address information technology (IT) as well as industry-specific operational technology (OT) systems.

Our cyber security services and solutions cover:

- **Organizational and technical gap assessments**: Supports you to achieve compliance with cyber-related regulations and standards according to your needs. Current emerging standards include IMO Resolution MSC.428(98), DNV GL’s Cyber secure class notation, ISO/IEC 27001, NIST Cybersecurity Framework, TMSA3, GDPR, etc.). Our cyber security experts engage with your onshore personnel and offshore crews to check written and informal standards established within your company and on board vessels.

- **Cyber risk assessment**: Our interdisciplinary teams engage with your onshore personnel and offshore crews to identify and address your cyber security risks via various levels of assessment, ranging from a high-level self-assessment via an app in My Services on Veracity to more detailed assessments tailored to your specific business risks. We identify gaps in your defence and countermeasures, both preventative and reactive, for IT as well as OT systems. Our aim is to help you create and maintain a strong and cost-effective cyber risk management.

- **Assessment of ships in operation**: We provide cyber security assessment and testing onboard your vessels, to identify lack of awareness of crew or procedural implementation as well as technical vulnerabilities.

- **Cyber security improvement**: Using systematic assessment techniques, we help you efficiently close cyber security gaps by supporting the development of improvement plans addressing systems, the human factor and management procedures.

- **Training**: Our (online) classroom training covers threats, incidents, regulations and threat prevention lessons. Our e-learning solution can be performed on board or in the office, so your crews can address pivotal aspects of any cyber security system - covering the human factor.

- **Social engineering tests**: In order to measure the awareness level of staff and crew, we can provide measurements from penetration testing using social engineering and phishing techniques.

- **EU GDPR**: DNV GL helps you achieve compliance with the EU General Data Protection Regulation (GDPR) through gap and improvement projects.

- **Incident response drills**: In order to be prepared for the worst, DNV GL executes tabletop drills to train and verify cyber security incident response both on vessels and in the office.

- **Penetration testing**: Testing the robustness of your barriers is essential to ensure that your assets are secure. Our penetration testing offers comprehensive and effective validation of your systems and procedures.

- **Verification for newbuilds and ships in operation**: Our class-independent maritime advisory experts assess, follow up, coordinate and support required improvements throughout the complete life cycle of a vessel towards the compliance with DNV GL’s Cyber secure class notation or letter of compliance for other classed vessels. Independently, DNV GL’s ship classification experts execute the certification.

- **Verification of components and systems**: Independently from the type approval process, our advisory experts assess, follow up, coordinate and support required improvements throughout the complete life cycle of components and systems towards the compliance with DNV GL’s Cyber Secure Type Approval Class Program.

- **ISO/IEC 27001**: Independently from the certification process, we assess and support you to improve your existing documentation and help you prepare for certification.

A proven cyber security partner

DNV GL’s class-independent advisory services combine traditional IT best practices with a deep understanding of the maritime industry and the operational technology employed. Our team of local and international experts draw on extensive knowledge and experience in a number of relevant areas, including ethical hacking, risk management, maritime operations and human factors. This helps ensure all testing and the suggested mitigation measures are tailored to the specific needs of our industry as well as your own particular needs.