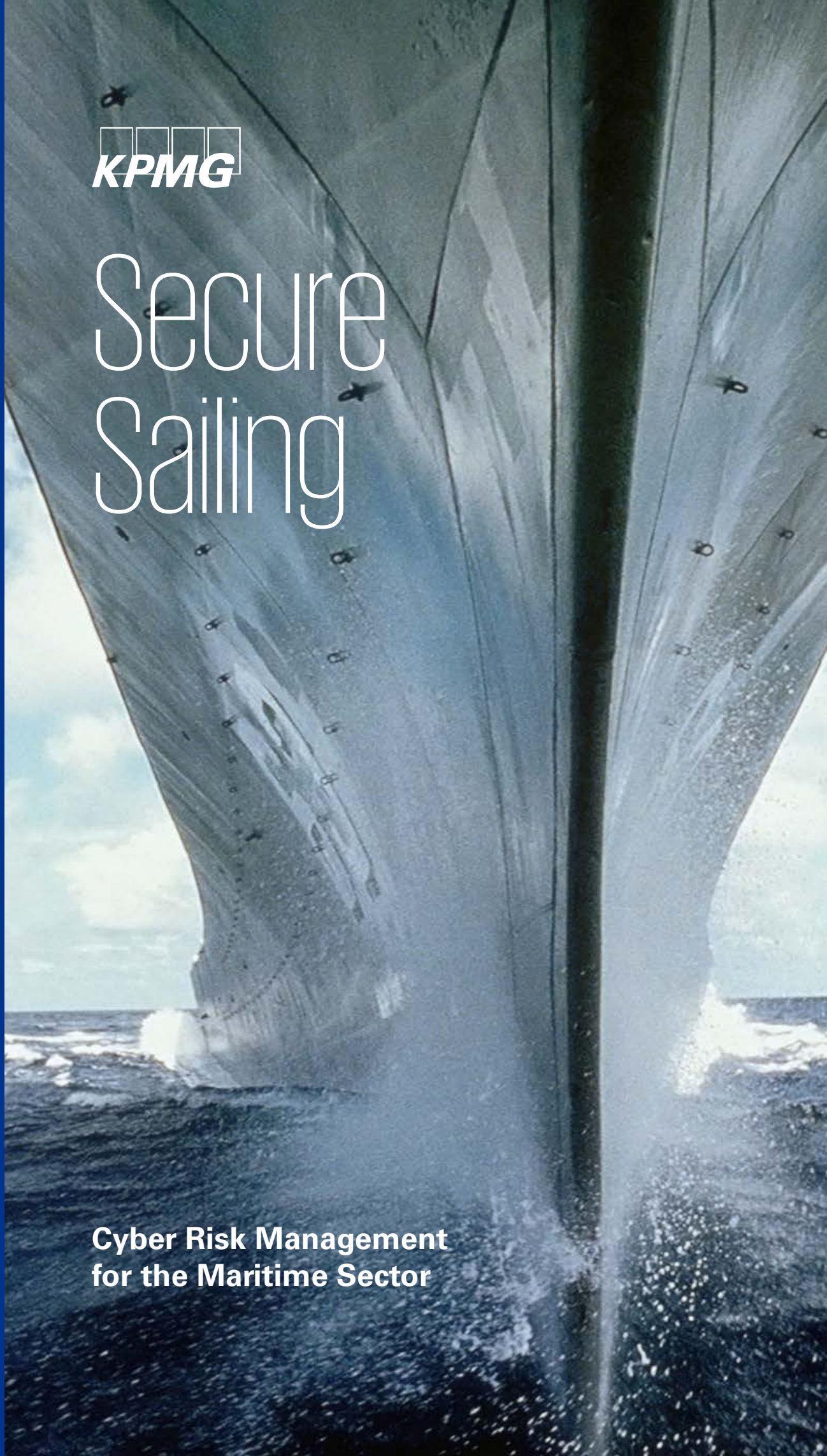


KPMG

# Secure Sailing

**Cyber Risk Management for the Maritime Sector**

# Welcome on board

The maritime sector is on the verge of a digital disruption. Digitalization is increasingly considered one of the key solutions to the many significant challenges the sector is facing, ranging from overcapacity, low margins, regulatory pressure, and lack of efficiency, to new digital demands from customers. Although digital transformation of the maritime sector is still in its infancy, it's safe to assume that digitalization will have a major impact on operations and existing business models in the years to come.

The Industrial Internet of Things (IIoT) is the new generation of technology innovation. The benefits from digitalization have already been manifested by early adopters, and we expect the sector adoption of new digital solutions will accelerate significantly going forward.

But fast-moving changes do not come without risk. Industrial automation and control systems, that were once isolated and deemed secure, are increasingly being connected to corporate networks and the Internet. Individual devices across enterprise Information Technology (IT) and Operational Technology (OT) networks – from smart digital equipment and tools to navigation, engines and more – will present potential new pathways to cyber attacks and incidents on your vessels.

In addition, regulatory requirements will come into play too. The International Maritime Organization (IMO) demands ship owners and managers to have incorporated cyber risk management into ship safety by 2021. Lack of compliance with these requirements may lead to increased insurance process, port access denial and even detention of ships, meaning huge financial losses for their owners.

To be able to make a safe and secure transition to the new connected digital market, you need to be able to manage risk in a consistent and transparent way.

# Cyber Risk Management

KPMG offers various solutions that help you manage your cyber risk in the way that is intended in, for example, the IMO *Guidelines on Maritime Cyber Risk Management* and the BIMCO *Guidelines on Cyber Security Onboard Ships.*

## Identify

*No single maritime IIoT landscape is ever the same. Do you understand the real risks for your environment?*

To be able to identify and manage risks and turn them into business advantages, you first need to understand your connected landscape and identify the most relevant threats and highest risks for your environment.

KPMG can assist you in getting to know your environment and threat landscape by:

- performing assessments to identify crown jewels and relevant threat actors for your organization and fleet
- finding potential attack paths towards your crown jewels
- identifying important components in your environment by determining potential impacts and risks
- assess the cyber maturity of your organization and fleet

*Our team has extensive knowledge in identifying the relevant risks for your organization.*

KPMG SOLUTIONS:

**CYBER RISK QUICKSCANS**
**FULL CYBER ASSESSMENT**
**FLEET RISK MANAGEMENT**
**CONTROL DEEP DIVES**
**ADVANCED RESILIENCE ASSESSMENTS**

## Protect

*Sufficiently protecting your environment is important. Have you implemented proper protection?*

Once you understand your maritime IIoT landscape and the impact and risks of the different systems within, you can take appropriate measures to protect it where relevant.

KPMG can assist you in improving the protection of your environment by:

- defining targeted areas where increased protection is required
- assessing protective measures by performing configuration reviews, controls designs and performing on-site inspections of physical security
- training staff on becoming more security aware
- assessing protection and resilience measures by performing advances penetration tests

*We can help you to assess and improve the maturity of your protection: our professionals have even performed penetration tests on live environments.*

KPMG SOLUTIONS:

**FULL CYBER ASSESSMENT**
**FLEET RISK MANAGEMENT**
**CONTROL DEEP DIVES**
**ADVANCED RESILIENCE ASSESSMENTS**
**STAFF CYBER SECURITY TRAINING**

## Detect

*No system is ever 100% secure. It's not a question if you will get hacked, but when. And then you want to know it.*

Having identified and designed the controls and measures to protect your environment, it is important to monitor them. By monitoring network traffic, logs and end-points, you can better detect cyber incidents.

KPMG can assist you in implementing and assessing the relevant controls for detection by:

- analyzing maritime IIoT network traffic for malicious behavior
- training staff to identify cyber incidents using our real simulated environment
- assessing processes around detection
- assessing detection controls by performing penetration tests and red teaming exercises

*With our global experience in the maritime sector, we can help assess these technical and non-technical controls.*

KPMG SOLUTIONS:

**CONTROL DEEP DIVES**
**CONTINOUS CONTROL AND COMPLIANCE MONITORING**
**ADVANCED RESILIENCE ASSESSMENTS**
**STAFF CYBER SECURITY TRAINING**

## Respond

*The first hours after detection of a cyber incident are vital. Do you know what to do when a cyber incident hits?*

When an incident happens, getting back to business as usual is key for your business continuity and safety. Hence, cyber response processes should be 'second nature' for your organization.

KPMG can assist you in responding to cyber incidents by:

- training staff to respond to cyber incidents using our real simulated environment
- assessing and designing cyber response capabilities
- teaming with you in cyber response at an instance's notice with our cyber hotline
- performing risk and security assessments to identify further potential impact to your fleet

*Our global team of incident responders can help you gain control over the situation during the first hours of an incident.*

KPMG SOLUTIONS:

**STAFF CYBER SECURITY TRAINING**
**INCIDENT RESPONSE SIMULATION AND ASSISTANCE**
**FLEET RISK MANAGEMENT**

## Recover

*After an incident occurred, stakeholders will need answers. Are you able to provide them?*

After the heat of the incident is over, and business is as usual, it is time to gain an understanding of the situation and evaluate the current security measures to prevent similar incidents in the future. At this stage you will need to answer stakeholder questions about the incident and identify lessons learned.

KPMG can assist you in recovering from cyber incidents by:

- performing a cyber investigation to determine the impact and extent of the incident, including actionable recommendations to strengthen your cyber resilience
- performing security assessments to identify further attack vectors
- perform maturity assessments to identify areas of improvement

*Our wide base of services enables us to help you recover from an incident, and minimize the change of it happening in the future.*

KPMG SOLUTIONS:

**INCIDENT RESPONSE SIMULATION AND ASSISTANCE**
**ADVANCED RESILIENCE ASSESSMENTS**
**CYBER RISK QUICKSCANS**
**FLEET RISK MANAGEMENT**

## A safe harbor

# KPMG and maritime

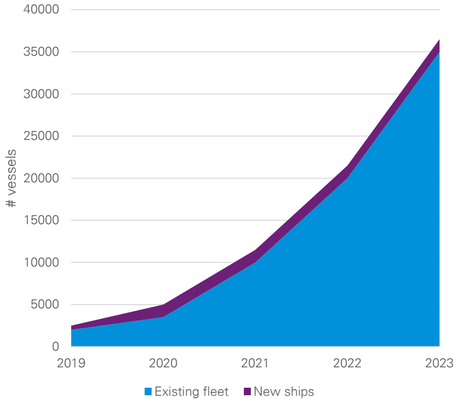
KPMG takes a sustained, modular, risk-based approach to help organizations with a successful integration of maritime IT and OT equipment and security. We have extensive knowledge on sector standards from e.g. IMO, BIMCO and NIST. Our experts leverage their vast experience in securing maritime IIoT to help you on your journey.

KPMG has been working on securing such systems since 2006, looking at various important aspects of technology, processes, governance and people. As such, we can adjust our offerings to the maturity of your organization. About to set sail with security? We will focus on manual documentation reviews and stakeholder interviews to gather information, supplemented with selected technical spot-checks.

Or are you aiming to sail high wind on security? We can automate aspects of our services, such as providing real-time risk management, continuous control monitoring of passively analyzing network traffic to locate malicious traffic or unexpected communications. Together with you, we determine the best way to navigate.

Of course, we understand the delicateness of maritime OT environments. We take special care on Health, Safety, Security and Environmental issues and operate with a focus on your business continuity.

**Increase in amount of Connected Vessels in 2019-2023**




Digitization and connected shipping will prominently be focused on transforming the existing fleet, which means that old and new technology will become connected. We have seen such digitization trends in other sectors and leverage those experiences for the maritime sector.

*Graph: McKinsey & Kongsberg Digital, 2018*

# Proven solutions

KPMG has assisted many organizations with their security challenges in dozens of projects, on almost all continents, both on- and offshore.
Our solutions have proven their value many times.

## Are you about to set sail...

**CYBER RISK QUICKSCAN**
Gives an overview of your biggest risks and the cyber maturity of your organization. We conduct a risk and maturity assessment based on procedural, human and technological factors.

**FULL CYBER ASSESSMENT**
Provides a better sense of the robustness of your overall security posture, and enables you to perform deep dives where they are relevant. We assess cyber security governance, risk management, IT and OT resilience, personnel and regulatory compliance efforts and give recommendations on improvement based on our experience and benchmark data.

**CONTROL DEEP DIVES**
Delivers a better sense of the robustness of your countermeasures and identifies gaps for improvement. We check your controls against our baselines and perform technical deep dives such as configuration reviews, penetrations tests and network traffic analysis.

**STAFF CYBER SECURITY TRAINING**
The staff on board is one of the most important factors in both defense and response. We deliver tailored education on cyber risks, do's and don'ts as well as indicators of potential cyber incidents in order to help you staff in safeguarding your valuable vessels and systems.

## ... or sailing high wind.

**FLEET RISK MANAGEMENT**
KPMGs Digital Risk Management solutions tailored to your fleet. As you try to balance investment with actual risk reduction, a comprehensive and quantified method to consistently assess and address the main risks across your portfolio of vessels will justify the cost of control. In addition, it helps you in complying with mandatory cyber risk management regulations (e.g. IMO).

**CONTINUOUS CONTROL AND COMPLIANCE MONITORING**
Provides real-time insight in any emerging cyber risks on board, plus timely notification when follow-up is needed. Automated control monitoring increases the level of control and compliance while leveraging the stream of data that your systems generate.

**ADVANCED RESILIENCE ASSESSMENTS**
Going deeper than the deep dive, we perform a full resilience assessment or red team exercise on selected attack vectors. We test and exploit like an advanced and persistent threat actor would do.

**INCIDENT RESPONSE SIMULATION AND ASSISTANCE**
Our real simulated environments and scenario-based training will let your staff learn and experience how to respond to cyber incidents – ranging from a quick exercise to a full-day realistic roleplay.

## Why KPMG?

KPMG has been working on securing OT environments since 2006, from testing RTUs to performing security audits on entire DCS and SCADA systems. During that time, we have seen numerous devices, environments, vessels, countries and platforms: our experts are even HUET and BOSIET certified.

We recognize the challenge of trying to secure legacy control systems that were not designed for security in a connected environment. That is why KPMG member firms are working with key vendors to build cyber security into their systems, from process controllers to robotics, so you can ensure a more resilient architecture. Drawing from industry expertise and strong market presence, KPMG can benchmark your cyber security with that of other clients in the maritime sector. We use deep OT and IT domain expertise and cyber risk management with cross-functional business expertise – including financial management, change management, organizational design and more. Our experts work closely with clients to create a unique maritime cyber security strategy and architecture that minimizes risk and supports your organization's mission within a stable, safe and predictable environment.

Partnering with KPMG ensures that you will get the KPMG quality with concise presentations and reports, and effective assistance, helping your enterprise to become future-proof. KPMG cyber experts operate internationally: we have an international network in over 155 countries which means we can provide the highest level of technical expertise both globally and as a local partner.

## Contact us

For more information on our Maritime Cyber Security Services, please contact one of our professionals or visit us at **kpmg.com/cybersecurity**


Arne Helme
KPMG Cyber, Norway
T +47 406 39 507
E Arne.Helme@kpmg.no

Thijs Timmerman
KPMG Cyber, Norway
T +47 477 18 865
E Thijs.Timmerman@kpmg.no

Ronald Heil
KPMG Cyber, The Netherlands
T +31 651 36 9785
E Heil.Ronald@kpmg.nl

Arno Sevinga
KPMG Cyber, The Netherlands
T +31 682 55 5387
E Sevinga.Arno@kpmg.nl