Lessons learned from other regulatory changes

In recent years, organizations in the maritime sector have experienced several changes in the external regulatory environment. Examples of such regulations were the implementation of the IMO's Low Sulphur regulation and the EU's General Data Protection Regulation (GDPR).

The latter also carried an additional financial risk of up to four percent of the total global revenue of the organization in case of non-compliance. In hindsight, there are many valuable lessons to learn from the implementation of GDPR that are highly relevant to the implementation of the IMO guidelines for cyber security in the maritime sector.

GDPR went into effect in May 2018. The regulation has changed the way in which organizations process personal data of their customers and employees, and how they interact with their business partners. For many organizations, the cost of GDPR compliance by far exceeded the allocated budgets, and did not necessarily result in full compliance with the regulations. Often, maturity of the organization's ability to handle the compliance risk, the short timespan before the regulation went into effect, and underestimation of the complexity of the tasks were contributing factors.

> "The key failure for many organizations was their one-sided focus on closing gaps found using different kinds of regulatory compliance gap assessments."

Due to the lack of strategy and understanding of the compliance risk landscape, many organizations did not address the question of what would be an acceptable risk level for their organization. What is good enough?

In addition, organizations started too late with addressing the consequences of non-compliance with the regulations. They underestimated the efforts needed to meet their compliance requirements. Only some had the right resources and skills available in their organization. Simultaneously, there were too few resources available in the market to close the competences gap because too many companies were in the same situation and looking for the same expertise.

The key failure for many organizations was their one-sided focus on closing gaps found using different kinds of regulatory compliance gap assessments (goals), instead of addressing their organization's continuous need for change in order to sustain acceptable compliance risk levels over time (values). They focused on "quick-fixing" the problem instead of enabling longtime, sustainable solutions for/to their business.

The IMO 2020 Low Sulphur regulation provides an additional example of how postponed adoption of new regulations might have a negative impact on risk as well as on costs. The IMO 2020 was announced during IMO's Marine Environment Protection Committee (MEPC) session in London late October 2016. The significant cut in allowed global sulphur emissions from 3,5% to 0,5% m/m meant that the industry needed to act in order to stay compliant. That said, the past time tells that the industry decided to sit on the fence until they "needed to act", hoping that the deadline would we pushed further into the future. The result, not surprisingly, has been an increase in prices and a lack of availability of scrubbers, as the uptake quadrupled in 2018. Limited capacity at yard slots left the late adopters in an even more troublesome position as they suddenly lack space for installing their scrubbers.

Combining leading positions

We can help you navigate safely through these challenges, enabling you and your company to reap the full rewards of connecting your vessels to the cloud and turn data into value.

KONGSBERG develops industry-leading technology that can be utilized for measuring, monitoring and correlating all types of maritime data. KONGSBERG offer an open digital ecosystem that helps clients unlock the value of their data.

KPMG has global expertise on cybersecurity advisory and digital risk management for critical sectors like maritime. KPMG develops digital risk management solutions that bring together their award-winning advisory practices, methodologies and industry benchmark data.

By combining leading positions in these areas, KPMG and KONGSBERG want to provide the maritime sector with innovative digital services to address existing and future cybersecurity risks.

Contacts

For more information about the transformation of your maritime cyber risk management practices and the immediate benefits of KPMG's and KONGSBERG's solutions for your organization, contact us or visit us at www.kpmg.com/no or at www.kongsberg.com/kdi

Vigleik Takle
SVP Maritime Digital Solutions
Kongsberg Digital
T: +47 488 40 870
E: vigleik.takle@kdi.kongsberg.com

Jan-Sigurd Sørensen
VP Maritime Digital Solutions
Kongsberg Digital
T: +47 930 33 219
E: jan-sigurd.sorensen@kdi.kongsberg.com

Arne Helme
Partner, KPMG
T: +47 406 39 507
E: arne.helme@kpmg.no

Thijs Timmerman
Senior Manager, KPMG
T: +47 477 18 865
E: thijs.timmerman@kpmg.no

CREATE. | CRT114423

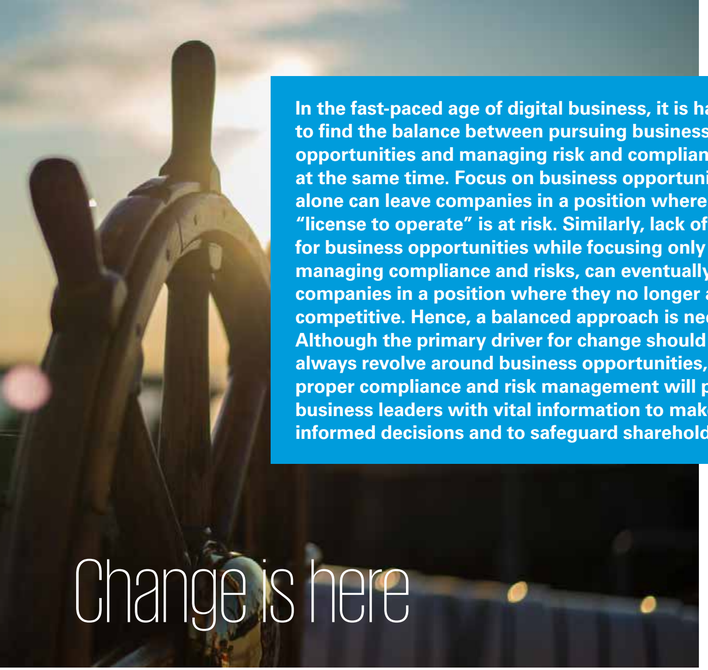
KPMG

KONGSBERG

Maritime license to operate at risk?

Balancing digital business opportunities and cyber risks effectively

kpmg.no/cyber



In the fast-paced age of digital business, it is hard to find the balance between pursuing business opportunities and managing risk and compliance at the same time. Focus on business opportunities alone can leave companies in a position where the "license to operate" is at risk. Similarly, lack of pursuit for business opportunities while focusing only on managing compliance and risks, can eventually leave companies in a position where they no longer are competitive. Hence, a balanced approach is needed. Although the primary driver for change should always revolve around business opportunities, proper compliance and risk management will provide business leaders with vital information to make well-informed decisions and to safeguard shareholder value.

Change is here

The digitalization wave has hit the maritime industry – and 2018 has been a turning point. While discussions around benefits and challenges have been going on for years, 2018 has shown an increase in actual investments. In addition, regulators and class societies are taking an increasing role in steering direction of the industry.

The digitalization wave has hit the maritime industry – and 2018 has been a turning point. While discussions around benefits and challenges have been going on for years, 2018 has shown an increase in actual investments. In addition, regulators and class societies are taking an increasing role in steering direction of the industry.

In the maritime community, it is commonly accepted that digitalization will have a major impact on operations and existing business models in the years to come. This belief has also been manifested by the investor community; over the past year, a major uplift in external funding into maritime tech startups was seen – from approximately 200 MUSD in 2017 to approximately 500 MUSD in 2018[1]. The number of companies delivering digital solutions to the maritime market is growing at a record pace[2].

Safety has always been a key driver in regulations of maritime operations. With increased digitalization, ship safety becomes increasingly dependent on IT and OT security. The International Maritime Organization (IMO) has already taken action and given ship owners and managers until 2021 to incorporate cyber risk management into ship safety. Owners run the risk of having ships detained if they have not included cyber security in the ISM Code on safety management onboard ships by 1 January 2021.

Similarly, classification societies increasingly focus on continuous safety and cyber security in the maritime industry. Several class notations around cyber security have recently been released, aiming to help ship owners and operators in protecting their assets from cyber security threats.

In a recent survey[3], 83 percent of business executives rate cyber security threats as a significant risk to organizational growth. However, when cyber is omitted from the digital business value chain, a trust ecosystem is not delivered, and a significant commercial opportunity is missed. Thus, cyber risks need to be addressed in order to achieve success.

1. Maritime Trend Report, Danish Ship Finance and Rainmaking, 2019.
2. KDI Maritime Software Landscape, 2019.
3. KPMG Consumer Loss Barometer, 2019.

The maritime sector operates in a complex environment

While many talk about "digital disruption" and a "paradigm shift" focusing on the long term effects, very few actually offer guidelines on what it requires from those organizations to succeed, managing both potential benefits and the subsequent risks.

With a rapidly changing risk landscape comes the challenge to stay up to date and make the right choices. The lack of sufficient cyber expertise has become increasingly visible in the last few years. Not only by means of various incidents, but also in the proliferation of sector-specific conferences, round tables and peer group meetings addressing the subject. The lack of expertise could make the sector more vulnerable, if not incapable of, dealing with the high pace of the current digitalization combined with new types of regulatory pressure.

Both new and existing fleets will have technology on board that will need to last for years. Because most IT and OT systems have a different lifecycle than the vessel and the machines they interact with, it is challenging to keep them secure in the future. This means that "secure by design"-principles will translate to the ability to design something that can be secured over a long lifespan.

> "A lesson learned in the approach towards GDPR, is that many organisations started too late."

The maritime sector has not always been able to keep cyber maturity on par with the degree of digitalization. A similar trend has been seen before in the oil and gas sector, where offshore installations and onshore plants were not designed or commissioned securely. It took the sector more than 10 years to manage system lifecycles in a proper way. The sector has ultimately embraced security as a leading principle in their focus on safety.

In regards to security, time is a complicating factor. First, technology and vulnerability exposure change significantly during the lifetime of a vessel. In an asset-heavy industry such as the maritime sector, one cannot just roll out technical improvements or perform massive updates on software across a business line. Intertwined IT and OT will need dedicated attention and planning – even physical access may be a challenge as systems are placed in distant vessels. It implies that maintenance on IT and OT systems may need to be aligned with expensive dock-time, or that proper remote access management needs to be in place in order to control that only the vendor will be able to perform updates.

Second, defined deadlines have been given by e.g. IMO on their resolution. Time to start designing and implementing a lightweight cyber risk management framework is running out. Clients and class societies are demanding improvements within a short timeframe, which makes it difficult to prioritizing 'doing it right' over 'doing it quickly'. A lesson learned in the approach towards GDPR, is that many organisations started too late. This caused panic, short-term decisions and excessive costs. After the deadline, however, it lead to apathy and eventually to a loss of benefits due to insufficiently anchored work. It shows that timely planning helps in longer lasting realization of benefits.

Just getting in external expertise and making a big leap will not entirely solve the maturity issue. From the implementation of GDPR, it has been learned that not only the one-off compliance activities are of importance, but also that embedding processes behaviour is vital. Without a proper way to maintain and continuously reprioritize cyber risk related efforts that may have been started, their benefits will vanish.

It can be challenging to validate whether or not your organization is addressing the most critical elements. The questions to ask yourself next Monday morning are:

- Do you have a clear digitalization strategy and vision on your future digital business models?
- Do you have control over the security risks that come with your digitalization strategy?
- Do you have the right people on board to fulfill your ambitions successfully?

How to navigate safely on the digital journey

In a fast-paced age of digital business, finding the right balance between business opportunities and its accompanying risks is not easy. Navigating through these new digital waters requires new skills and processes in the organization. Business, security and compliance needs go hand in hand in order to maintain sea-worthiness in the digital era. For that, the following guiding principles can be deduced.

Pursue business opportunities with risk in the back of your head

Companies need to be pragmatic in their approach towards digitalization and in understanding the accompanying risks. The license to operate must never be at stake. It is important to understand and recognize the resources and capabilities within the organization and complement that with third party solutions where needed. This approach makes an organization focusing on its core business and exploring new possibilities. Adding third party services and resources will add complexity and reduce control, making it more important to have a holistic approach towards risk management.

Invest in the building the right skills and capabilities in the organization

It will involve "re-talenting" the workforce, identifying critical roles and understanding the required capabilities. For many organizations, a cultural shift will be needed to build cyber risk management into all digitization efforts. At the end of the day, secure by design means that the workforce has a security mindset and embeds that mindset into everything they do.

You cannot do this alone; it is not your core business

Accomplished market actors will be working to provide solutions and fulfill parts of your needs on a continuous basis. By doing so, the organization moves away from remediating one-off gaps, towards a more dynamic approach where emerging risks are continuously addressed.

Start in time and start small

The task of tackling the cyber challenge seems large and complex, but if you start in time and divide the task into smaller pieces, it becomes manageable for even small organizations. The best advice we can give is to get started today, and not wait for the perfect solution or the time to address everything in one go.