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’s ability to handle regulatory compliance gap assessments (goals), instead of understanding the consequences of non-compliance. The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business.

The IMO 2020 Low Sulphur regulation provides an additional example of non-postponed adoption of new regulations. The IMO 2020 Low Sulphur regulation goes into effect in October 2020, providing an additional example of how regulatory compliance gap assessments (goals) might have a regulatory impact to the business in short term as well as on costs. The IMO 2020 Low Sulphur regulation is a significant cut in the environmental emissions from ships and will require a significant investment in new machinery and equipment. The latter also carried an additional financial risk of up to four percent of the total global revenue of the organization’s ability to handle regulatory compliance gap assessments (goals), instead of understanding the consequences of non-compliance. The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business.

The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. The lack of strategy and plan has an immediate benefit of the organization’s ability to handle regulatory compliance gap assessments (goals), instead of understanding the consequences of non-compliance. The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. Due to the lack of strategy and plan, many organizations did not address the question of what risk level was acceptable for their organization. What is good enough? What is the right level of risk to accept? What is the risk appetite of the organization’s ability to handle regulatory compliance gap assessments (goals)?

The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. The lack of strategy and plan has an immediate benefit of the organization’s ability to handle regulatory compliance gap assessments (goals), instead of understanding the consequences of non-compliance. The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. Due to the lack of strategy and plan, many organizations did not address the question of what risk level was acceptable for their organization. What is good enough? What is the right level of risk to accept? What is the risk appetite of the organization’s ability to handle regulatory compliance gap assessments (goals)?

The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. The lack of strategy and plan has an immediate benefit of the organization’s ability to handle regulatory compliance gap assessments (goals), instead of understanding the consequences of non-compliance. The key failure for many organizations was that the focus was on closing gaps found using inefficient methods, and the lack of strategy and plan contributed to these failures. They focused on “quick-fitting” instead of providing long-term, sustainable solutions to their business. Due to the lack of strategy and plan, many organizations did not address the question of what risk level was acceptable for their organization. What is good enough? What is the right level of risk to accept? What is the risk appetite of the organization’s ability to handle regulatory compliance gap assessments (goals)?

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/vdi.
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. For many maritime companies, 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 long are a compelling risk to their stakeholders, be it internal or external. Although the primary driver for change should always revolve around business opportunities, ignoring compliance and risks, can be detrimental to a company’s profitability and overall reputation. 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.

In the maritime sector, digitalization has become a significant component of the industry’s transition to a more modern, efficient, and sustainable future. The digitalization wave has hit the maritime industry – and 2018 has been a turning point. In the maritime community, it is commonly accepted that the maritime sector has not always been able to keep cyber maturity on par with the degree of digitalization. A similar trend has been witnessed in the oil and gas sector where offshore installations and onshore plants were not designed or commissioned secured. It took the sector more than 10 years to manage system lifecycles in a proper manner. The sector has ultimately embraced security as a leading principle in their focus on safety.

In regards to security, time is a complicating factor. Offshore installations and onshore plants were not designed with new types of regulatory pressure. 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. The task of tackling the cyber challenge evolves with time and is 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.

The maritime sector operates in a complex environment. Changes here are not always welcomed by everyone. The digitalization of the maritime sector has created a new landscape, where the traditional ways of doing business are being challenged. The digitalization wave has hit the maritime industry – and 2018 has been a turning point. In the maritime community, it is commonly accepted that the maritime sector has not always been able to keep cyber maturity on par with the degree of digitalization. A similar trend has been witnessed in the oil and gas sector where offshore installations and onshore plants were not designed or commissioned secured. It took the sector more than 10 years to manage system lifecycles in a proper manner. The sector has ultimately embraced security as a leading principle in their focus on safety.

In regards to security, time is a complicating factor. Offshore installations and onshore plants were not designed with new types of regulatory pressure. 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. The task of tackling the cyber challenge evolves with time and is 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.