

Cyber compliance without the extra burden:

a procurement view of maritime cyber risk

124

Cyber compliance is no longer just an IT concern. It is now part of everyday marine purchasing, supplier management, and operational risk control. The real challenge is not simply meeting new requirements, but doing so without increasing cost, paperwork, and workload. For maritime teams, the next priority is to make cyber compliance practical, repeatable, and manageable.

Marine purchasing teams are used to working under pressure. They need to control costs, secure reliable suppliers, avoid delays, support vessels, and keep documents in order. Today, they face one more challenge: cybersecurity compliance. For many teams, the concern is not whether cyber security matters. The concern is how to manage it without adding another heavy layer of cost, paperwork and manual effort.

What happens when compliance becomes part of everyday purchasing?

Cyber risk management is no longer a future issue for shipping. IMO guidance, IACS UR E26 and E27, class expectations, insurance questions and customer requirements are all pushing the industry in the same direction. Compliance is becoming part of normal maritime business. But for shipowners, managers and purchasing teams, the practical question is clear: how can we meet these requirements while keeping operations lean?

This question matters because vessels are now highly connected working environments. Navigation systems, satellite communications, engine monitoring, maintenance platforms, cargo systems, remote access tools and supplier portals all create digital connections. These connections support efficiency, but they also create new weak points. CYTUR's 2026 Maritime Cyber Threat White Paper found that recorded maritime cyber incidents increased from 408 in 2024 to 828 in 2025, a rise of 103%. For procurement teams, this is no longer only an IT issue. It is a supplier risk, a contract risk, an operational risk and a compliance risk.

Can cyber compliance become a cost problem of its own?

The challenge is that most companies do not have unlimited cyber experts, budgets or time. Many maritime teams are already managing cost pressure, crew workload, technical operations and regulatory reporting. If cyber compliance becomes another manual checklist exercise, it can quickly





A better approach starts with one simple principle: cyber compliance should reduce risk without creating unnecessary work. Marine buyers do not need to become technical cyber specialists.

create duplicated supplier questionnaires, repeated document requests, unclear responsibilities and slow onboarding. In other words, poor cyber compliance processes can become a cost problem themselves.

A better approach starts with one simple principle: cyber compliance should reduce risk without creating unnecessary work. Marine buyers do not need to become technical cyber specialists. But they do need a practical way to decide which suppliers, systems and contracts require closer attention. Not every purchase carries the same risk. A connected navigation system, remote monitoring platform or satellite service should receive a deeper review than a low-risk consumable item.

Are we asking the right questions before the contract is signed?

This is where purchasing teams can use three practical questions:

- ① Which suppliers or products create the highest cyber risk?
- ② Can supplier cyber evidence be collected once and reused instead of requested again and again?
- ③ Who owns the cyber risk after purchase, and does this process reduce workload, or simply add another checklist?

These questions help turn cyber compliance from a broad concern into a manageable purchasing process. They also help companies focus resources where they matter most. High-risk systems can receive deeper checks. Lower-risk purchases can move faster. This risk-based method supports both compliance and efficiency. It avoids treating every supplier the same and reduces unnecessary workload for teams that are already stretched.

Where is the evidence when the auditor asks for it?

Supplier evidence is especially important. Regulations and class requirements increasingly expect companies to show what has been checked, how risks are managed and who is responsible. In practice, this evidence is often scattered across emails, spreadsheets, PDF certificates and internal folders.

That creates extra work for procurement, technical, IT and compliance teams. It also makes audits more stressful than they need to be.

A more structured process can reduce this burden. When supplier cyber information is collected in a consistent way, kept up to date and linked to the relevant vessel, system or contract, teams spend less time chasing documents. When risk status is visible, managers can make decisions faster. When responsibilities are recorded clearly, there is less confusion during audits, incidents, renewals or supplier reviews. AI-assisted tools can accelerate this further — automatically screening supplier documents, flagging outdated certificates and summarising risk status without manual review.

What is the real cost of unmanaged cyber risk?

Cyber security is often seen only as an additional expense. But unmanaged risk creates hidden costs: vessel downtime, delayed operations, duplicated supplier reviews and last-minute compliance work. The goal should be lean compliance — meeting requirements with minimal manual effort while improving safety and resilience. For marine procurement, lean compliance means clear supplier criteria, risk-based prioritisation, reusable evidence and audit-ready records. It is about making the right information available at the right time.

Marine purchasing has always helped protect the vessel by choosing reliable products and suppliers. In the connected ship era, that responsibility now includes digital reliability as well. The strongest companies will not be those that create the most documents. They will be those that make cyber compliance practical, repeatable and efficient.

Can cyber resilience be secure and manageable at the same time?

For shipping companies, the next step is not to add more complexity. It is to build a simpler way to understand supplier cyber risk, prove compliance and reduce unnecessary workload. In a market where every cost and every hour matters, cyber resilience must be more than secure. It must also be manageable.