



The Fragmentation Problem in Maritime Compliance

Scaling compliance amid escalating complexity

For maritime chartering, operations, finance, and compliance leaders

Marcura 2026 Report

Acknowledgements

This report draws on conversations with industry experts and practitioners working across maritime compliance, people navigating the exact pressures this report describes.

We are extremely grateful to everyone who gave their time and shared their experience.

Industry contributors:

Bianca Knight, General Manager, Commercial Claims, Pacific Basin Shipping

Mike Gerasymov, Global Head of Corporate Risk, Enesel Group

Fieke Nijland, VP, Legal Counsel, Emirates Shipping Line

Cecilia Müller Torbrand, CEO, Maritime Anti-Corruption Network

Marcura contributors

Andrei Grigoras, SVP, Compliance Solutions

Taher Afridi, Deputy Chief Compliance Officer

Al Fyvie, Compliance Officer and Deputy MLRO for MarTrust

Abigail Gries, Global MLRO for MarTrust

Saurish Nandi, Solutions Head for Compliance for ShipServ

Contents

01 Foreword:

Andrei Grigoras on the compliance burden facing maritime teams and the case for shared infrastructure.

02 The new sanctions reality:

Diverging sanctions regimes, stricter enforcement expectations, and a shadow fleet of over 1,500 vessels operating in opaque networks, many linked to sanctioned trade.

03 The wider risk universe:

Payment fraud running three to five times higher than traditional banking, tightening ESG standards, and persistent port-level corruption across 150 countries.

04 Compliance pressure points:

Survey findings: 82% report growing compliance demands, 86% worry about undetected risks, and onboarding costs reach \$3,500 per counterparty.

05 The fragmentation problem:

Ten screening platforms producing divergent answers on the same counterparties. No mechanism to share what's been learned. Mistakes repeating across the ecosystem.

06 AI in maritime compliance:

What AI can realistically deliver, where hype exceeds reality, and why the future is hybrid.

07 Compliance as shared infrastructure:

Verification performed once, recognised across workflows, reinforced by collective intelligence.

08 Marcura unified compliance:

How 25 years of transaction data and operational platforms provide the foundation for a unified compliance ecosystem.

01 Foreword

Andrei Grigoras,
SVP, Compliance Solutions, Marcura



A compliance officer starts Friday morning with hundreds of regulatory alerts in her inbox. Three jurisdictions updated their lists overnight. A charterer needs sign-off on a vessel by noon. Procurement wants to know why a long-standing supplier is suddenly flagged. Finance is querying a bank account change.

By Wednesday, some cases are cleared, but many remain. Each unreviewed alert carries liability and time-pressure. By Thursday evening, one question lingers: “Did we miss something?”

This is the repeating cycle for maritime compliance teams, driven by three avoidable failures.

First, irrelevant alerts create noise. Many hits are low value: fuzzy name matches, stale records, or minor media mentions. They drown out the few that matter. Quieting that noise frees scarce human attention for real risk.

Second, when an alert is relevant, assessing context and impact is complex, but it should not be. Sanctions are not binary. Some are blocking, others restrictive or licence-based. Many create secondary exposure through financing or nationality. A hit alone does not reveal the consequence for a specific transaction. An automated impact assessment should combine policy, operational context, sanction type, and data confidence to prioritise work and surface the regulatory outcome. Humans retain judgment for material cases.

Third, impact must be visible where the business works. Bank account changes, agent nominations, supplier RFQs, and vessel sign-offs require impact-aware alerts embedded directly into chartering, procurement, and payment workflows so consequences are clear and the right action follows.

Fragmentation adds to these challenges. Multiple systems and standards recreate the same work across the maritime chain. The fix is not more alerts, but smarter sequencing: reduce noise, score impact first, and embed outcomes into operations with governance and audit trails. That is how compliance becomes predictable protection and the industry moves from fragmented effort to shared infrastructure.

When compliance is embedded into day-to-day workflows, commercial teams regain speed, onboarding and payment friction fall, and scarce expertise focuses on higher-value work. The results are measurable: faster deal execution, lower operating cost, stronger counterparty and bank confidence, and a clearer link between compliance investment and performance.

Can new approaches turn “not another compliance tool” into “can I get a clear answer without all this work?” This report is an invitation to that conversation. After 25 years serving maritime, Marcura has developed perspectives on what works and what the industry must build together. I hope these insights prove useful as you navigate what lies ahead.

02 The New Sanctions Reality

Sanctions regimes that once operated in close alignment are now diverging in scope, priorities and enforcement. Expectations have shifted from reacting to breaches to preventing them. A shadow fleet of more than 1,500 vessels operates in opaque networks, many linked to sanctioned trade, though not all are designated. This is not temporary. Organisations treating it as such are most vulnerable.



1,500+ vessels
Estimated size of the shadow fleet

No golden standard

When US, UK and EU sanctions regimes coordinated closely against Russia in 2022, compliance teams built frameworks around a shared risk perimeter. Though never fully harmonised, parallel listings reduced uncertainty. The assumption followed: screen against US OFAC and apply conservative controls, and exposure across the main Western regimes would generally align.

That assumption is weaker today. Divergence now reflects differences in strategy, enforcement and jurisdiction, not just timing.

The EU has continued expanding its Russia-focused sanctions and is now advancing a 20th

package to tighten pressure further, including measures that could effectively end the G7 oil price cap and impose a full ban on maritime services for Russian tankers. The US followed its own priorities, maintaining strict liability and secondary sanctions while placing greater emphasis on Iran alongside Russia.

Why does this matter in practice? Because companies face multiple regulators applying different rules to the same transaction. Trading in dollars places you under OFAC jurisdiction. Employing EU nationals creates EU obligations, even if based in Asia. Compliance exposure is no longer singular. It is layered.

“Today you have sanctions regimes from different authorities that don't always align. As compliance officers, we have to decide which regimes we're going to abide by, in addition to, of course, adhering to our own regulatory authority's requirements.”

—
Senior compliance officer,
global commodities trading house



Indirect sanctions exposure

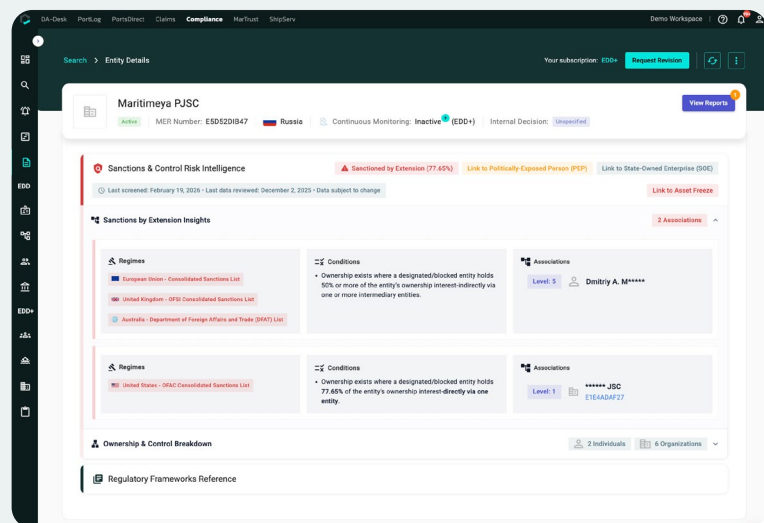
Enforcement no longer stops at the named counterparty. It extends through ownership and control. A company may not appear on a sanctions list yet still be restricted, effectively sanctioned by extension, if it is owned or controlled by a designated person.

For maritime organisations, this risk sits beneath the surface. Vessels are held through layered structures and SPVs while charterers may operate through newly formed entities. A counterparty's "full style" identifies the contracting entity but rarely shows who ultimately owns or controls it. Cargo interests and traders can sit behind corporate chains not visible in the contract.

Ownership rules and secondary sanctions increase that exposure. An organisation can face penalties not for dealing directly with a

sanctioned party, but for enabling a transaction involving one indirectly.

Screening the named counterparty is no longer enough. Compliance requires identifying ultimate beneficial owners and mapping control structures. Without that visibility, risk remains hidden until regulators uncover it.



The enforcement shift

Regulators have changed their expectations. Enforcement no longer focuses only on clear violations. Organisations are expected to identify and manage sanctions risk before transactions occur. Authorities are pursuing willful blindness cases more actively, holding organisations accountable for control gaps that should have detected exposure. Ignorance is not a defence when risk was discoverable. Static or periodic screening is increasingly insufficient in an industry that demands continuous oversight.



The shadow fleet

A parallel shipping infrastructure now exists to move cargo that cannot move through legitimate channels. Figures from Clarksons Research put the size of the shadow fleet at 1,578 ships.

According to [analysis](#) by the Center for Strategic and International Studies, Russia's shadow fleet transports an estimated [3.7m barrels of oil a day](#), representing 65% of Russia's seaborne oil trade, and generates an estimated \$87bn (£69bn) to \$100bn (£80bn) annual revenue.

Vessels linked to the shadow fleet are typically poorly maintained tankers with complex ownership structures, often layered through shell companies and special purpose vehicles designed to obscure who controls them. They operate beyond Western reach, outside conventional insurance and classification. Beyond the compliance risk they pose, these ageing vessels pose a genuine physical risk to valuable assets being legally transported through the same waters.

For charterers, the risk is tangible. Charter a vessel that has touched sanctioned trade, and OFAC may designate it tomorrow. Your cargo is stuck on a blacklisted ship with no clean way out.

Regulators tighten the net

Regulators have responded with force. In 2025 alone, more than 700 vessels were sanctioned across US, EU, and UK actions. Panama struck almost 70 ships from its register. Barbados removed 46. Comoros began purging vessels falsely claiming its flag.

Yet the fleet reconstitutes. Sovcomflot tankers, stripped of Liberian registration, reappeared under Gabon's flag within days. Gambia and Sierra Leone have emerged as new havens. A study carried out by S&P Global in late 2025 found more than 370 vessels flying a false or fraudulent flag, up from 223 vessels at the beginning of the year.

Top 10 flags of shadow vessels



Image source: TankerTrackers.com

Significant international efforts, led by the US and UK, are intensifying to disrupt it using legal powers to board and seize tankers. The shadow fleet is facing a significant challenge and heightened risk, but it's not over.

The underlying incentives remain unchanged. Sanctioned oil still needs to move, and buyers still want it. Third countries without Western restrictions have stepped into the gap, their economies expanding as they become conduits between sanctioned states and global markets. Tracing whether a counterparty contributes to a sanctioned economy now means following money through places designed to hide it.

A permanent condition

Russia triggered the current intensity, but sanctions have settled into a permanent instrument of foreign policy. Iran remains heavily restricted. Venezuela shows that enforcement can tighten without warning, though a recent announcement authorizing US companies to buy, sell, transport, store and refine Venezuelan crude oil suggests a more widespread easing of sanctions could be on the horizon. Future conflicts will generate fresh designations.

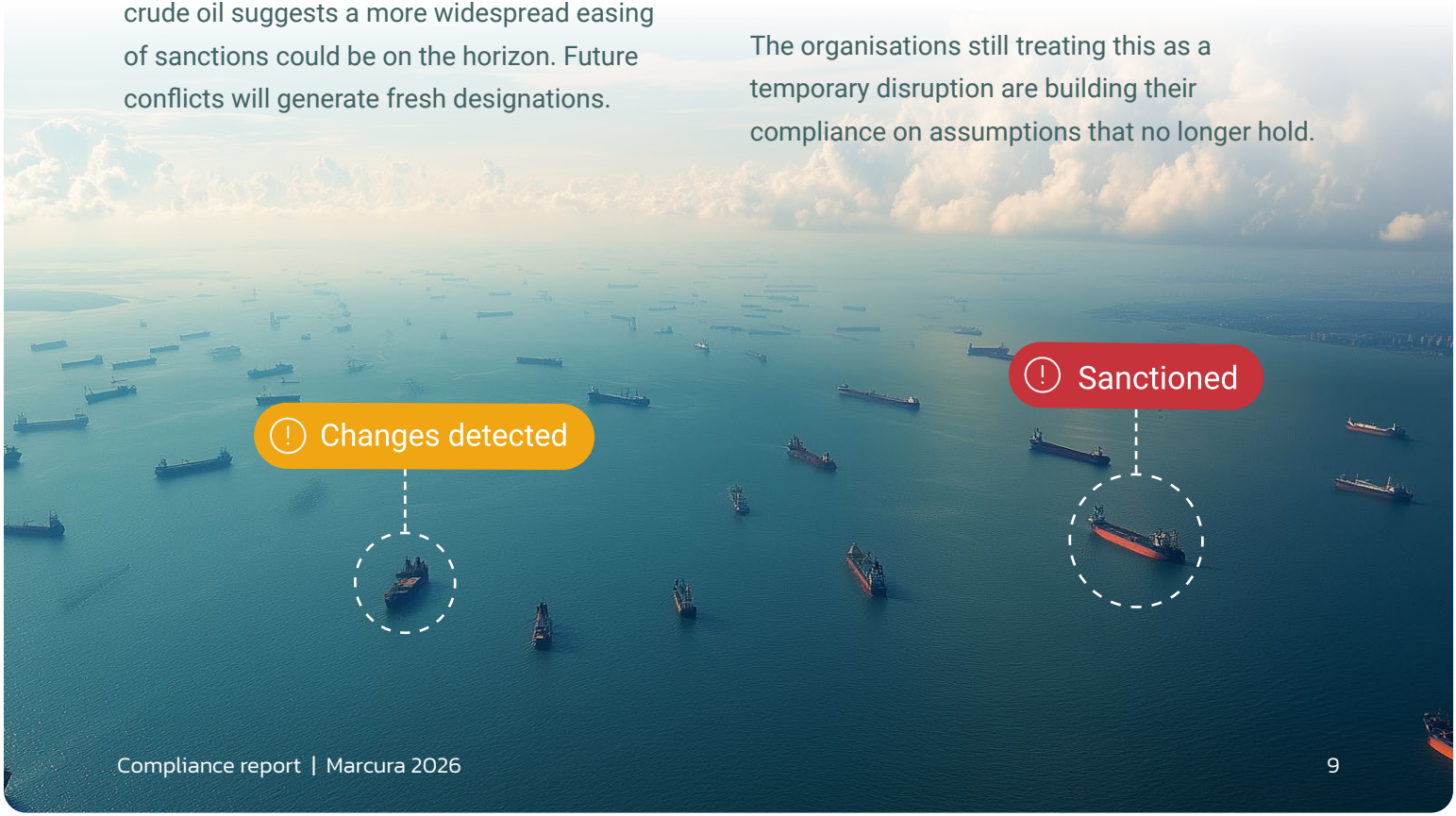
The pattern is clear: regulators will continue expanding the definition of prohibited conduct to close gaps as actors adapt. Complexity will increase, not decrease, with each enforcement cycle. Secondary sanctions will expand. Beneficial ownership verification expectations will tighten.

For legitimate operators, exposure is now twofold.

The first is regulatory: any brush with the shadow fleet risks fallout that cascades through insurance, banking, and counterparty relationships. The consequences can be existential including exclusion from the US dollar payment system if designated by OFAC, reputational damage from association with sanctioned activity, and financial penalties including multi-million-dollar fines and asset seizures.

The second is physical: over 1500 poorly maintained vessels operating outside classification and insurance frameworks share the same sea lanes as legally operated assets. The shadow fleet poses a direct risk to the vessels your organisation depends on.

The organisations still treating this as a temporary disruption are building their compliance on assumptions that no longer hold.



! Changes detected

! Sanctioned

03 The Wider Risk Universe

The sanctions landscape is only one part of a much broader risk environment maritime organisations are now expected to manage. Payment fraud, cybersecurity threats, supplier compliance, environmental obligations, and anti-bribery controls are converging into a

single operational reality. Each introduces its own regulatory and financial exposure, but they increasingly draw on the same data, rely on the same verification processes, and fail in the same places when those foundations are weak.



Payment fraud

Business email compromise (BEC) and payment fraud targeting maritime runs three to five times higher than traditional banking when adjusted for transaction volume.



ESG and supplier obligations

Growing demand for suppliers to evidence compliance with ISO, ISM and Scope 3 emissions. New regulations may require organisations to switch suppliers to remain compliant.



Anti-bribery and corruption

The Maritime Anti-Corruption Network has documented over 70,000 corruption related reports from more than 1,000 ports across 150 countries. The lack of unified standards for assessing anti-bribery and corruption compliance is an industry-wide challenge.





Payment fraud risk

According to DNV's Maritime Cyber Priority 2024/25 global report, nearly a third of maritime professionals reported at least one cyber-attack in the twelve months to October 2024, up from 17% over the previous five years. For compliance teams, payment fraud is the most pervasive and measurable threat in the broader cyber-risk universe.

Business Email Compromise (BEC) and payment fraud targeting maritime organisations runs three to five times higher than traditional banking when adjusted for transaction volume. The reason is structural. Shipping combines high-value transactions with decentralised decision-making and limited bank verification infrastructure. Vendor relationships are transactional rather than long-term, counterparties frequently change bank details for legitimate reasons, and vessel schedules create pressure to process payments fast.

3.4 billion

phishing emails sent daily

"Approximately 1.2% of all emails sent are malicious, amounting to around **3.4 billion** phishing emails per day globally."

Source: SSL Insights

Attacks have evolved from crude phishing to deep-learning approaches that mimic legitimate vendor communication patterns, timed to align with known vessel schedules. Adversaries can now craft compromise strategies designed to evade known detection models. The result is an arms race where algorithmic defences alone cannot guarantee protection.

Attackers use supply chain intelligence to craft convincing narratives, targeting individuals with authority to approve transfers up to an established threshold but limited verification processes.

The warning signs: bank detail change requests arriving shortly before scheduled payments, communications referencing specific vessel names or charter details, urgency framing around operational pressures.

Maritime port agents are particularly vulnerable. Most are small operations using free email providers which lack security and privacy measures for business correspondence. Compromising these accounts requires minimal sophistication; a cloned website can be created in seconds using free AI tools.

Approval thresholds compound the problem. Where retail banking might require secondary approval for transactions exceeding a few hundred dollars, maritime organisations processes five-figure payments at first authorisation. Once funds clear, the money is gone for good.

Payment fraud illustrates the limits of fragmented controls. When verification is inconsistent, responsibility defaults to individuals operating under time pressure. Once funds move, recovery is rare, and the evidentiary burden shifts to proving controls existed rather than preventing loss in the first place.

Some maritime operators have responded by embedding verification directly into payment workflows, introducing centralised account validation, controlled change management, and last-mile screening before funds are released. At sufficient scale, these controls also surface coordinated fraud patterns that isolated systems cannot detect.

Marcura's payment infrastructure embeds controls at multiple points in the transaction.

\$2.4 million

in customer funds protected in 2025

In 2025 alone, the system prevented five fraud attempts, protecting approximately \$2.4 million in customer funds. Over nine years, that record extends to roughly 190 prevented attempts worth \$10 million.

The impact of payment fraud goes beyond just the direct monetary loss, causing further loss in repeat attacks, loss of trust with customers, regulator fines, and reputational damage, among others. The real damage is far more significant and could be existential in nature.



! Updating payment details

! Incorrect details provided

! Unapproved supplier



ESG and supplier standards

Supplier vetting has traditionally focused on financial and sanctions risk. That scope is expanding fast under regulatory pressure that now touches environmental compliance, hazardous materials management, and supply chain emissions, a convergence the maritime industry has yet to fully absorb.

4,000 hours
IHM administration per year

The Hong Kong Convention, which entered force in June 2025, requires every vessel trading internationally to maintain an up-to-date Inventory of Hazardous Materials throughout its operational life. One seven-vessel fleet estimated they were spending more than 4,000 hours per year on IHM administration alone, a burden that traditional

Embedding environmental standards in procurement

Marcura's IHM as a Service flags hazardous materials before orders are placed and automates the collection of Material Declarations and Supplier Declarations of Conformity, turning what was previously a reactive documentation chase into a predictable, auditable workflow. d'Amico Group, managing more than 70 vessels from Rome, Mumbai, and Singapore, digitised their IHM and supplier-vetting processes through ShipServ.

"Marcura's ShipServ gives us the tools to acquire documentation earlier—material declarations, supplier declarations of conformity, all gathered inside the platform. It's easy to manage because we have categorisation and standardisation of the process."

Francesco Leboffe, Procurement Manager,
d'Amico Shipping Group

- Inventory of hazardous material
- Supplier vetting and assessment
- Regulatory compliance

IHM Report

Your traded products that have registered IHM



Description	Status	Hazard Type
Epoxy (Finish)	Complete	Batteries
Lithium Pack	Complete	Nuclear
Emergency Lifebuoy	Complete	Lead
Polyurethane Sealant	Complete	Paint and coatings (anti-fouling)
Reflective Safety Ring	Pending	Nuclear
Hull Protection	Pending	Paint and coatings (anti-fouling)

Scope 3 blind spots

Scope 3 emissions represent an even larger challenge. These indirect emissions, embedded in the goods and services a company procures, can account for up to 60% of a shipping company's total carbon footprint. Yet most organisations have minimal visibility into them. The same spare part carries a completely different emissions profile depending on where it was manufactured, how it was shipped, and how it will ultimately be disposed of.

The IMO's Net-Zero Framework, approved in principle at MEPC 83 in April 2025, introduces mandatory greenhouse gas fuel-intensity targets alongside a two-tier pricing mechanism. Ships missing the base emissions target would face charges of \$380 per tonne of CO₂ equivalent, while those meeting the base target but exceeding the stricter direct-compliance threshold would pay \$100 per tonne. These price levels have been proposed for the initial implementation phase, previously envisaged as 2028 to 2030, with final timelines and future rates subject to further agreement.

Formal adoption of the framework, originally expected in October 2025, has been deferred by one year, with member states continuing work to reach consensus on the final design.

Risk convergence

Suppliers must now demonstrate not only that they're free from sanctions exposure, but that they hold relevant ISO certifications, meet ESG criteria, and can evidence their own supply chain compliance. Owner-operators need documented proof that their ship managers are sourcing from suppliers who meet evolving standards, evidence that port authorities and insurers will increasingly demand. The question facing procurement teams is no longer "is this supplier sanctioned?" but "can this supplier evidence compliance with our environmental, safety, and governance standards, and can they do so at the point of transaction, not months later when the leverage has gone?"

Digital procurement platforms like Marcura's ShipServ are evolving to address this convergence. The opportunity lies in embedding compliance verification directly into sourcing workflows: hazardous material flags appearing before orders are placed, emissions estimates surfacing alongside pricing and lead times, supplier credentials verified once and recognised across transactions. The same structured data foundation that enables IHM compliance today can expand to support Scope 3 reporting, future environmental metrics, and whatever regulatory requirements emerge next.

Port	Status		
Port of Tanjung Priok Owner	OK	Today by	AK
Astrakhan Owner	Sanctioned	3 days ago	AK
Port of Ningbo-Zhoushan Owner	OK	30 Oct 2024	AK

Regulatory compliance

Confirmed

Towage	USD \$1,327.47
Agency Fee	USD \$13,275.79
Total	USD \$14,603.26

Vendor invoices

[AET-240274-2V \(Burger Poland Ltd. - Gdynia\)](#)





Persistent corruption risk

Since its founding in 2011, the Maritime Anti-Corruption Network (MACN) has documented over 70,000 corruption-related reports from more than 1,000 ports across 150 countries. In 2025 alone, MACN received 4,347 reports detailing instances of extortion, often described as "gratuities," which contravene international anti-corruption standards.

Some cases are starkly alarming. Former master Stephen Gudgeon told the BBC he was held at gunpoint at an Asian port after refusing to hand over cigarettes. "They took me ashore at gunpoint and I was locked up. I was photographed and fingerprinted, and I was interviewed by two officials in an empty room with just a chair, which I was locked into." Other situations are less dramatic but equally troubling, crew members facing demands for food stores, or small sums of cash.

The Maritime Anti-Corruption Network (MACN) remains the industry's primary body addressing

70,000

Corruption-related reports

corruption in maritime trade. Working alongside the IMO, which approved guidance on procedures against maritime corruption in May 2022, the network coordinates collective action across eleven countries. While the IMO provides procedural guidance on handling corrupt demands at the operational level, no unified framework exists for assessing counterparty ABC risk. Companies adopt their own question sets and interpret them according to what they consider material to their business.

This absence of standardisation echoes across every risk vector. Sanctions regimes diverge. Payment fraud detection varies by provider. ESG requirements shift by sector and jurisdiction. The compliance function finds itself managing a portfolio of distinct threats, each demanding its own processes, documentation, and proof of diligence, with little infrastructure connecting them.

The cost of corruption

Corruption in maritime trade carries costs that extend far beyond the port gate. MACN's Cost of Corruption Study puts a dollar value on the impact across the private sector, government, and society.

In Nigeria alone, a key case study for maritime import supply chains, the cost of corruption to the industry involved in importing food and bulk products exceeds USD 162 million per year, adding close to 15% to total transport and logistics costs. Per shipment, this amounts to USD 147,000 for grain and over USD 178,000 for petrol imports.

The indirect costs compound the picture.

Corruption-driven delays reduce Nigerian GDP by an estimated USD 204 million annually, cut customs revenue by USD 42 million, and eliminate more than 235,000 full-time equivalent jobs. Essential goods become less affordable to ordinary households, with corruption adding 1–2% to retail prices for grain and fuel.

The business case for collective action is equally clear. Under a zero-tolerance scenario, the cost of corruption to the maritime industry drops by over 62%, saving more than USD 100,000 per import shipment. GDP grows, customs revenues recover, and jobs are created.

Why Standardisation Alone Won't Fix Maritime Compliance

Cecilia Müller Torbrand,
CEO, Maritime Anti-Corruption Network (MACN)



Cecilia Müller Torbrand leads strategy and industry engagement at the Maritime Anti-Corruption Network (MACN), a collective action bringing together app. 230 global companies across the maritime value chain to address corruption as a shared industry risk.

“The Maritime Anti-Corruption Network (MACN) was founded around a simple recognition: corruption is a risk, and it is very hard to face it alone. Around fifteen years ago, a small group of maritime companies came together to ask whether they could gain by collaborating across the industry rather than trying to address the problem in isolation. That question is still at the core of what MACN does today.

“Today, MACN brings together companies across the maritime value chain. That value-chain perspective matters, because everyone has a role to play. For example, cargo owners, shipowners, crew managers and port agents all have operational impact. When those actors work toward one standard and one approach, that collective action itself can drive change.

“It is very easy for organisations to stay in their own box and focus only on what they can control internally. But if compliance programmes look only at colleagues and internal processes, and not at what customers, suppliers, and peers are doing, risks may be isolated without actually being mitigated.

“Third parties remain one of the biggest sources of corruption risk, yet due diligence is often a paper exercise. Questionnaires are sent out, policies are uploaded, and boxes are ticked. That may demonstrate effort, but it does not necessarily change behaviour.

“Standardisation is an important step in the process. Today, suppliers are asked to complete broadly the same due-diligence exercises repeatedly, across different platforms and with slightly different questions and phrasing. It's hard to ‘kill your darlings,’ but agreeing on a shared set of relevant questions would reduce duplication and make it easier for suppliers to engage meaningfully.

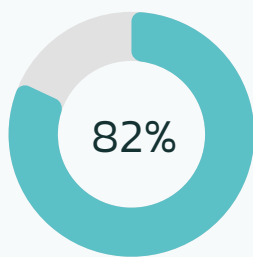
“But that level of standardisation on its own is not enough. Risk mitigation does not lie in how questions are phrased. It lies in what happens afterwards. If you want to change behaviour in high-risk markets, you need dialogue, trust, and engagement. You need to understand the pressures suppliers face when dealing with authorities, permits, and inspections. Sending a questionnaire alone will not achieve that.

“Incentives matter. Suppliers are repeatedly asked to invest time and effort in compliance without receiving anything back. Capacity building is still largely missing from due-diligence work.

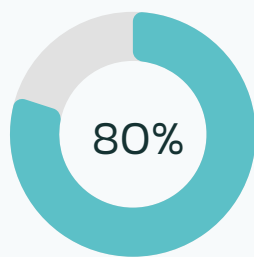
04 The Compliance Pressure Points

Marcura asked operations directors and senior maritime leaders about their compliance challenges. The responses reveal a workforce under strain, struggling to keep pace with regulatory change, losing time to manual processes, and increasingly aware of the gaps in their defences.

The Burden

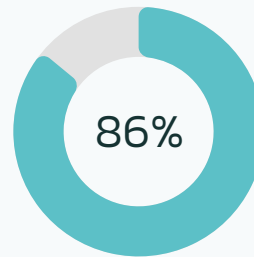


Say compliance is a growing demand in their role

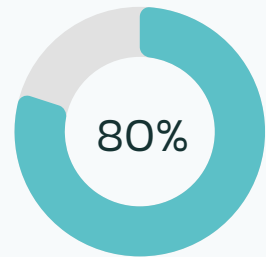


Find it hard to keep up with Financial Crime Compliance (FCC) changes

The Anxiety

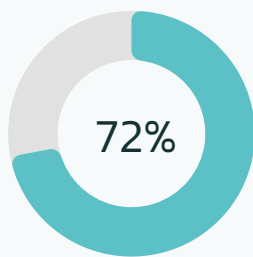


Are concerned about compliance gaps and undetected risks

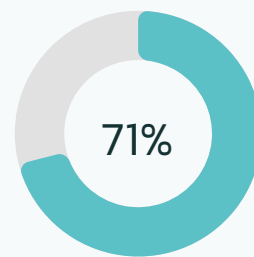


Cite siloed data and communications channels as a major efficiency inhibitor

The Drag



Struggle to complete all required KYC / FCC checks



Say manual due diligence consumes too much time

Technical barriers

- ✓ Absence of a unique, global, authoritative counterparty identifier, specifically
- ✓ Fragmented data processes
- ✓ Lack of data governance leading to inaccurate counterparty data

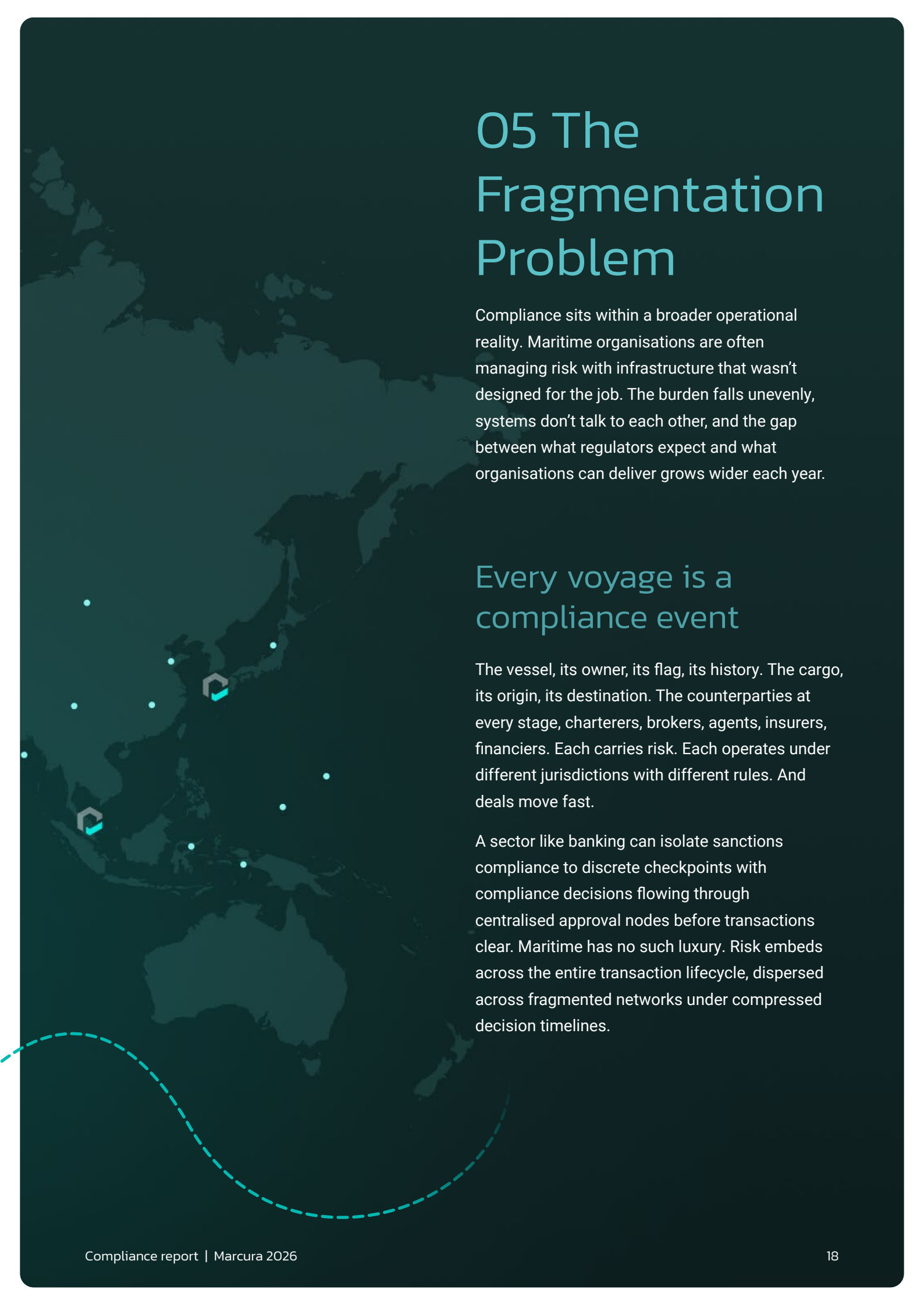
The hidden cost

\$1,500–\$3500

Estimated combined cost of onboarding and KYC per counterparty

The result

Organisations are struggling to manage sanctions risk in a way that is both effective and efficient.



05 The Fragmentation Problem

Compliance sits within a broader operational reality. Maritime organisations are often managing risk with infrastructure that wasn't designed for the job. The burden falls unevenly, systems don't talk to each other, and the gap between what regulators expect and what organisations can deliver grows wider each year.

Every voyage is a compliance event

The vessel, its owner, its flag, its history. The cargo, its origin, its destination. The counterparties at every stage, charterers, brokers, agents, insurers, financiers. Each carries risk. Each operates under different jurisdictions with different rules. And deals move fast.

A sector like banking can isolate sanctions compliance to discrete checkpoints with compliance decisions flowing through centralised approval nodes before transactions clear. Maritime has no such luxury. Risk embeds across the entire transaction lifecycle, dispersed across fragmented networks under compressed decision timelines.

When someone in the chain gets it wrong, the mistake doesn't stay contained. It cascades through the network as institutional knowledge rather than a controlled correction. Regulators hold all participants liable for that cascade.

Common compliance challenges

-  Difficulty obtaining due diligence data
-  Lack of single Platform focused on maritime
-  Lack of specialist Compliance talent and retention of talent
-  Lack of standard KYC processes and policy
-  Evidencing compliance to customers, investors and auditors
-  Heightened sanctions regulations
-  Manual and slow compliance processes
-  Due diligence on suppliers during onboarding
-  Keeping due diligence data up to date
-  Lengthy compliance checks slow down commercial activity and decrease
-  Opaque ownership, beneficiaries and UBOs

No orchestration layer

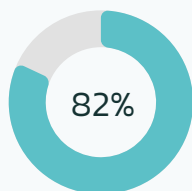
Organisations will often use several screening platforms, sanctions databases, beneficial ownership tools, vessel tracking systems, PEP and adverse media lists. But different platforms return different results on the same counterparty. One clears, another flags amber, a third returns inconclusive. What do you do when there's divergence?

The compliance team becomes the manual integration layer, piecing together a risk picture from fragments. The deeper issue is what these systems can't see. A name-matched search can appear clean while missing shell companies, obscured beneficial ownership, or vessel histories marked by extended dark periods. Sanctions evasion hides in corporate structures, not company names.

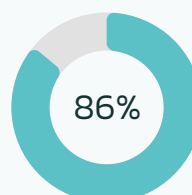
The talent squeeze

Specialist maritime compliance expertise is scarce and hard to retain. Compliance headcount cannot scale proportionally with complexity.

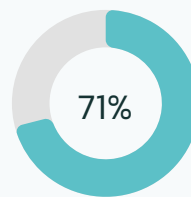
The work has shifted in character. Compliance teams now spend significant time proving they performed checks to insurers, banks, P&I clubs. Each wants evidence in different formats, against different standards. Teams are feeling the strain.



82% of maritime professionals say compliance is a growing demand in their role.



86% are concerned about compliance gaps and undetected risks.



71% report that due diligence administration is manual and takes time away from core responsibilities

Estimates put the combined internal resource cost of onboarding and KYC at \$1,500–\$3,500 per counterparty. In fragmented markets like dry bulk, where every other business opportunity requires onboarding someone new, the resource drain becomes structural.

Supplier fatigue

Fragmentation hits suppliers too. Vendors complete the same information requests repeatedly for every customer, different questionnaires, different formats, different portals. Questionnaire fatigue sets in. Forms get completed carelessly. Data quality suffers.

Each organisation runs its own checks. Each supplier answers the same questions dozens of times. The system demands maximum effort from everyone and delivers minimum collective benefit.

Knowledge doesn't travel

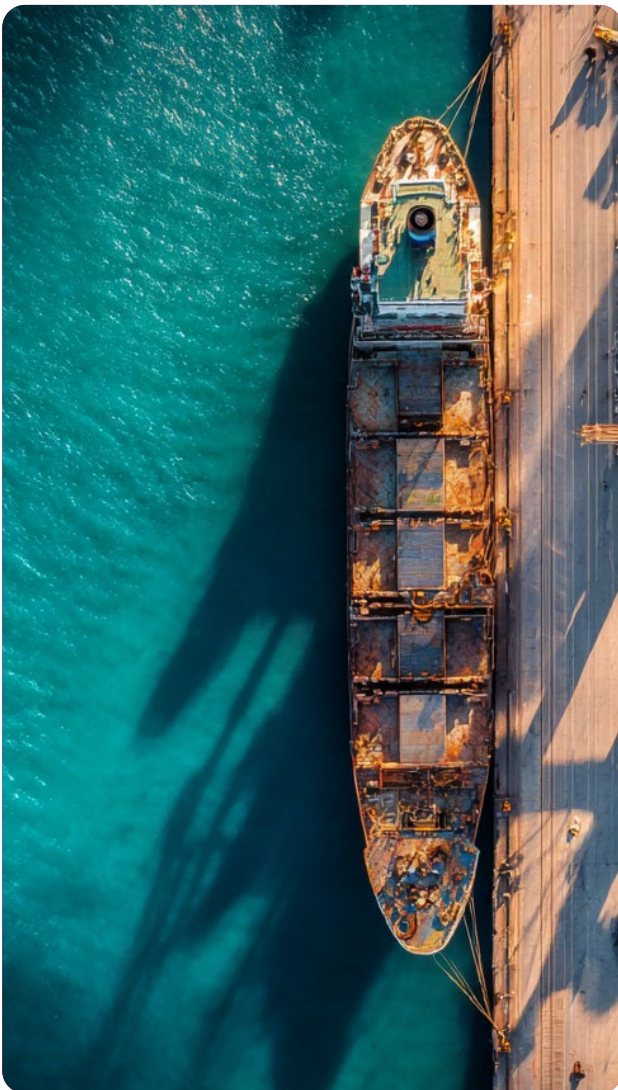
Organisations lack infrastructure to share what different teams have learned. Knowledge sits in silos with no mechanism for compliance insights to flow to colleagues who need them. Teams look at the same counterparty repeatedly without realising it.

"You have the compliance knowledge, the credit knowledge, the risk knowledge, the commercial knowledge. But they're all stored in different places, and we can't tap into that knowledge easily.

"The systems we use aren't good enough or agile enough to support knowledge sharing. We're hampered by our own databases and structures."

—

Senior compliance officer,
global commodities trading house



Across the industry, the pattern scales. The same counterparty gets vetted by dozens of organisations. When one discovers something, a compromised supplier, a fraudulent payment pattern, that intelligence stays locked inside their walls. The next organisation encounters the same threat and falls for it.

Industry bodies have made progress on specific vectors. MACN coordinates anti-corruption efforts. Classification societies maintain vessel standards. P&I clubs share claims data within their membership. But when it comes to commercial counterparty screening, organisations still largely operate in isolation, each bearing the full verification cost alone, mistakes discovered by one repeating at the next because there's no mechanism to share what's been learned.

The data to solve this problem already exists, scattered across thousands of transactions, port calls, and payments processed daily. The question is whether the industry can aggregate it into shared infrastructure that benefits everyone.

Finding the Sweet Spot in Compliance

Fieke Nijland, Vice President, Legal Counsel at Emirates Shipping Line



Fieke Nijland is Vice President, Legal Counsel at Emirates Shipping Line (ESL). ESL doesn't have a dedicated compliance department, but compliance is handled by a team that spreads across the legal and operations departments. They found a way to handle compliance screening efficiently at scale without building a large operation around it.

"Sanctions compliance used to be simpler. Twenty years ago, you knew which countries were off limits, you avoided them, and that was largely the end of it. Today the regulatory landscape is more complex. Libya, Syria, Russia, each conflict has added new sanctions territory to navigate.

"In container shipping, a single vessel might carry five thousand containers. So theoretically, you could have five thousand bills of lading, each with a shipper and a consignee. Some containers carry multiple cargoes from different parties.

"You only fully know who the shipper is when cargo is presented at the port. That leaves very little time to complete due diligence before containers are loaded. If results come back too late and a problem cargo is already aboard, you're into mitigation territory.

"Compliance is handled by a team across various departments. Escalation sits within my remit. There are very large shipping lines capable of doing screening themselves, which needs a lot of manpower. ESL believes in using technology driven solutions for this and sits in a sweet spot of company size where it makes sense to get a specialist involved.

"That's why we work with Marcura. We have a team in India who prepare the data from our bill of lading information. They send it to Marcura for screening, receive the results back, and analyse them. When something flags such as a potential sanctions match or a concern about cargo, it escalates to me and a few colleagues.

"What helps is that we can specify which sanctions regimes are relevant to us and the system is configured to filter out the rest. Whatever is sanctioned in Brazil is completely irrelevant to me because we don't call Brazil. Certain flags carry higher risk, certain jurisdictions need closer scrutiny, and the system reflects that.

"When I send a party for screening, there's a good chance Marcura has already screened them in the past for either ourselves or someone else. If I give Marcura an IMO number for a vessel I'm chartering, and it's a commonly used vessel in that trade, I can get a report relatively quickly, because they likely already have data on it.

"In the current regulatory landscape, Governments may impose sanctions, but it's companies and their financial partners who need to take steps to police them.

"That reality shapes how we think about compliance investment. Avoiding fines is one thing, but more than that, it's about maintaining the relationships and access that let us operate. Screening isn't an overhead cost, it's a condition of doing responsible business."

06 AI in Maritime Compliance

The compliance conversation cannot avoid artificial intelligence. The technology appears at every industry conference, features in every vendor pitch, and generates both inflated expectations and genuine uncertainty about where it can truly add value. What can AI realistically deliver? Where does hype exceed reality? And what are the risks of getting it wrong?

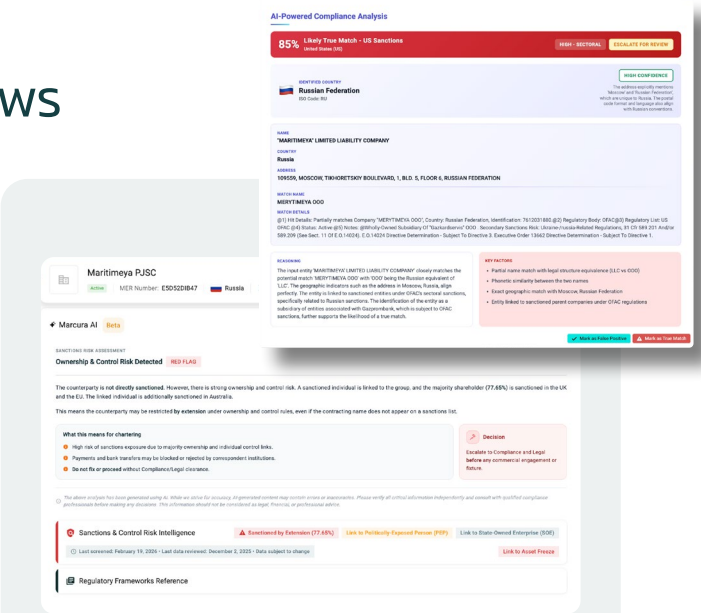
In operational settings, AI delivers the most value when applied to first-line triage and interpretation rather than final decision-making. Applied this way, it reduces noise, surfaces meaningful risk signals, and translates complex compliance outputs into language that non-specialists can act on—without removing human oversight from high-stakes decisions.



Practical applications in live compliance workflows

One practical use case is sanctions screening. When a counterparty generates hits across multiple regulatory lists, AI can assess the likelihood that the screened entity matches the sanctioned party, filtering out obvious false positives while escalating genuinely ambiguous cases for review. This approach preserves quality control while removing a significant volume of low-value manual work.

A second application focuses on accessibility. Operational teams frequently encounter compliance alerts without the context required to interpret them. A screen filled with red indicators creates anxiety but not clarity. AI-generated summaries can explain which regulatory regimes are triggered, why they matter, and what the practical implications are for an organisation operating under US, EU, or UK jurisdiction—without requiring deep compliance expertise at the point of decision.



The screenshot displays the 'AI-Powered Compliance Analysis' interface. At the top, a red banner indicates an '85% Likely True Match - US Sanctions'. Below this, the system identifies the 'IDENTIFIED COUNTERPARTY' as 'Russian Federation' and the 'COUNTERPARTY' as 'MARITIMEYA LIMITED LIABILITY COMPANY'. The interface provides detailed information about the company, including its address and legal status. A 'SANCTIONS RISK ASSESSMENT' section highlights 'Ownership & Control Risk Detected' with a 'RED FLAG'. The system explains the risk, noting that the counterparty is not directly sanctioned but is linked to a sanctioned individual. A 'What this means for chartering' section lists potential risks, such as high risk of sanctions exposure and payment/charter issues. The interface also includes a 'Sanctions & Control Risk Intelligence' section with links to further information and a 'Regulatory Frameworks Reference' section.

Marcura has implemented this approach in live compliance workflows, using AI to support alert triage and to present risk exposure in plain language to chartering, operations, and finance teams. The objective is not to automate decisions, but to ensure that decisions are made with clarity rather than confusion.

The hybrid future

Full automation is neither possible nor desirable. Regulators explicitly expect human judgment in high-stakes compliance decisions. Organisations that remove human review entirely are creating audit vulnerabilities rather than operational improvements.

The realistic future is hybrid: AI handling routine screening, anomaly detection, and risk quantification, with humans reserving judgment for ambiguous cases, emerging threat patterns, and decisions with material business or reputational consequences.

The competitive advantage goes to organisations that can efficiently deploy AI in the right form, at the right spot in the process, and within defined context and guardrails—then use that AI component to liberate human expertise from tactical screening work and redirect it toward strategic risk management: understanding emerging regulatory patterns, evaluating novel counterparty structures, and building institutional knowledge that survives regulatory changes and enforcement cycles.

Green light, red light: Enesel's journey towards compliance automation

Mike Gerasymov, Global Head of Corporate Risk at Enesel Group



Mike Gerasymov is Global Head of Corporate Risk at Enesel Group, with more than 20 years' experience across dry bulk and liner shipping. When he joined Enesel, he had the opportunity to reimagine the compliance function and set it on a journey towards full automation.

"When I joined Enesel, the compliance function was undergoing a radical transformation. I inherited existing processes and systems, but there was no compliance team in place. That created both an opportunity and a sense of urgency.

"Marcura supports our screening workflows. But there was still friction in terms of how requests got to them. In the old process, a broker would email counterparty information to our front line. A chartering manager would forward it to the vetting team. The vetting team would review it, check the entity names, then email it to Marcura. The process was manual and email-heavy, with multiple hand-offs.

"The first thing I built was an agentic AI chatbot. Staff can paste information like an email thread or a list of names into the chatbot interface. It then validates entity names, prompts if a legal suffix is missing, and structures everything into a clean list.

"A key benefit is that the chatbot shields users from frequent backend changes, which are often disruptive, even when they're positive. Our people use the same interface while we keep developing what sits behind it. All they notice is

that response quality improves and turnaround time shrinks.

"For now, the chatbot still hands off to Marcura by email, but we're working on an API integration to address that. The eventual goal is capturing information automatically from source systems, no human input required, just a green light or a red light delivered to the person who needs it. But that's a little way off."

"What's stood out working with Marcura is their willingness to listen and their readiness to learn from each other through innovation. That's underpinned by a shared understanding that continuous change in this space is inevitable.

"Compliance might be complex on one level, but it also consists of certain principles and criteria which can be described in natural language. Today, 80 to 95 percent of previously manual compliance work can be automated at minimal cost and with very limited software development expertise.

"The reasons full automation won't happen quickly aren't technical. They're human: trust, resistance to change, and the practical question of which projects to prioritise first.

"While compliance is a critical control function, it should not distract commercial teams from their primary role. The goal is to give them clear, well governed compliance decisions, enabling them to focus on safe and efficient trading within defined boundaries."

07 Compliance as Shared Infrastructure

Why fragmented compliance no longer works

A clear answer. That's what commercial teams need. Not ten platforms producing divergent results. Not weeks of onboarding for counterparties. Not compliance functions buried in tactical screening when they should be focused on strategic risk.

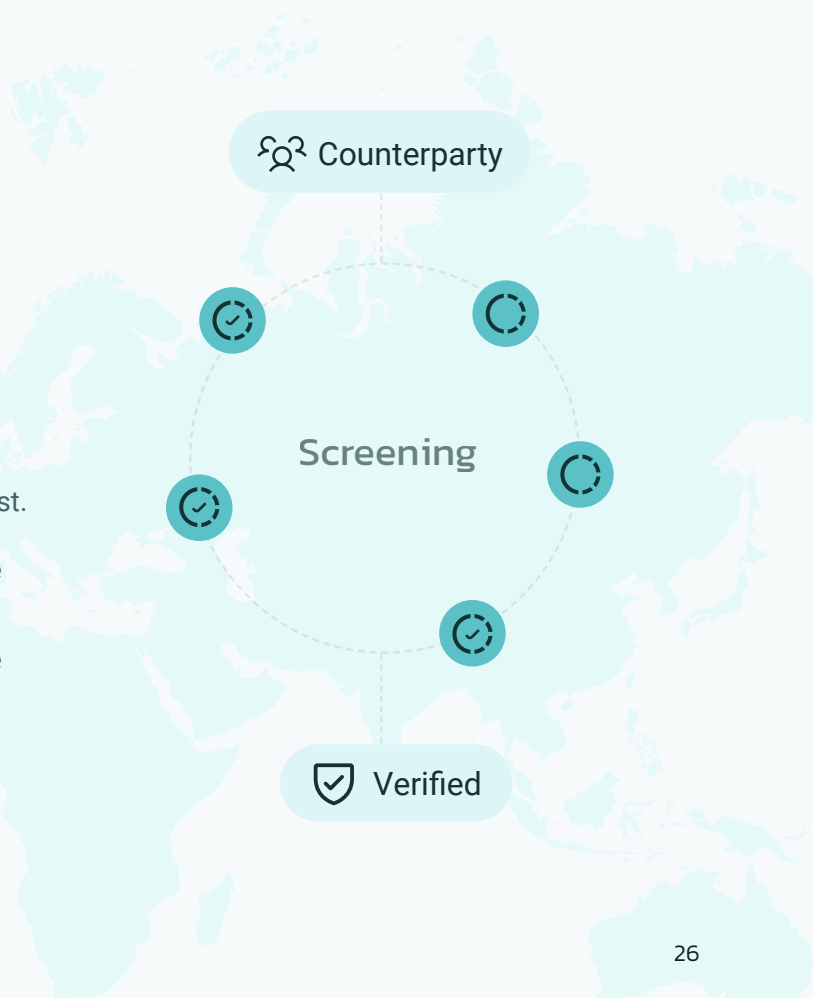
AI can accelerate individual workflows. It cannot solve the structural problem: every organisation building parallel verification infrastructure, bearing the full cost alone, learning nothing from what others have already discovered.

That requires something different. Compliance functioning as shared infrastructure. In a shared infrastructure model, compliance is no longer rebuilt independently by every organisation. Verification is performed once, recognised across workflows, and reinforced by collective intelligence that allows risks identified in one context to protect participants that contribute to it.

Operating Within a Trusted Ecosystem

Think of it as a walled garden extending from commercial chartering to procurement and through to payment. Anyone entering - ship supplier, trader, port agent, operator, charterer, owner - is screened before participation. Only when cleared do they trade inside, where every transaction starts from a position of verified trust.

Inside the perimeter, commercial teams operate at speed because the verification work has already been done. Outside, counterparties face a choice: complete rigorous onboarding once and carry that credential across the ecosystem, or keep duplicating paperwork for every new customer.



Removing duplication of work

Current models force everyone to repeat mistakes in isolation. A networked model builds institutional knowledge that survives across the industry. Counterparties verified once carry that verification across the ecosystem. A supplier onboarded to a common standard becomes available to every organisation subscribing to that standard. Protection extends to every participant without each organisation having to discover the same problem independently.

Siloed systems cannot detect patterns that span multiple transactions and counterparties. Screening integrated across an ecosystem catches what fragmented checks miss, ownership chains, related entities, transaction patterns that only become visible when data flows through a shared infrastructure rather than staying locked inside separate organisations.

Centralised change management

Bank account fraud succeeds because change requests slip through approval processes designed for legitimate updates. An email arrives requesting new payment details. The change looks routine. Funds transfer before anyone recognises the manipulation.

Centralised verification flips this: any change request triggers automatic verification through a direct call to the number held on file during original onboarding. Every change is suspicious until independently confirmed.



For the CFO:

Payment fraud carries quantifiable costs, funds lost, recovery efforts that rarely succeed, control failures that invite scrutiny. Sanctions violations carry exposure reaching hundreds of millions. The arithmetic favours prevention.



For the Compliance Officer:

Escape from tactical overload. Networked compliance shifts the burden to specialists, freeing internal teams for judgment calls requiring institutional knowledge.



For Commercial Teams:

Speed rather than impediment. Pre-verified counterparties mean the compliance function becomes invisible protection running in the background.



For Suppliers, Agents, and Vendors:

Liberation from questionnaire fatigue. A single compliance passport replaces duplicated onboarding for every customer relationship.



Where to start

Shared infrastructure doesn't require an all-or-nothing commitment. Organisations sit at different points depending on their risk appetite, internal capability, and how much of the compliance workload they want to retain.

At one end of the spectrum some may choose to use shared verification as a data source. Screening results feed your internal processes; your team applies policy and makes the call.

At the other end, organisations may choose subscribe to a standard policy with delegated execution through a managed service. The infrastructure screens, resolves alerts,

delivers a status. You retain authority over which policy you adopt; the operational work happens externally.

Most organisations sit somewhere between, and move along that range as needs evolve. Start with screening data. Expand to managed workflows for higher-risk counterparties. Shift toward fuller delegation as trust builds.

At no point does this increase your exposure. Each step improves data quality, process consistency, and documentation. What changes is how much operational work your team performs.

Scaling compliance, without scaling headcount

Bianca Knight, General Manager, Commercial Claims, Pacific Basin Shipping



Bianca Knight manages claims, dispute handling, sanctions compliance, and contract management at Pacific Basin Shipping, one of the world's largest dry bulk operators with more than 200 vessels.

"Our process used to be heavily PDF-driven. The team introducing the counterparty would get them to fill out a form with their details. That would go to the due diligence team making manual checks, then documenting the screening results, sharing them and storing them in a way that's auditable so you can show later that you've completed a due diligence process on this counterparty.

"When there was a sudden spike of sanctions in 2022, our manual process simply wasn't designed to cope with the increase in volume. Using the Marcura platform has allowed us to scale without adding to the team.

"Checks are done in the platform, and we can see the results the entire time. We're able to configure the system to reflect how we want to manage our risk and there's an audit trail on what's submitted when which is important for us. It's also allowed us to push down onboarding to the teams who are introducing the counterparties and shift the compliance decision making to a smaller team trained in making those decisions.

"We have internal decision makers that provide compliance approvals within each function, overseen by a small team that

includes myself and the risk team in Hong Kong. We've been able to move away from just collecting forms, making sure they're filed, a lot of manual workflow processes, to actually making the compliance decisions and considering scenario analyses rather than spending a lot of time on admin.

"Looking across the industry, everyone's running their own checks with their own risk matrix, their own risk appetite, and their own interpretations. There isn't an industry-wide standard for what we consider acceptable due diligence.

"As jurisdictions increasingly go their own way on regulations it's going to become increasingly difficult to remain compliant unless the industry comes together to agree on a common baseline for due diligence. There needs to be transparency for there to be trust in it. We would need to understand who did the check, when it was done, what it was checked against. I think that would allow you to have a shared platform or a more transparent platform everyone's able to rely on.

"Where we see the sticking point is often compliance with banks and payments being delayed while they investigate counterparties that we have already screened and cleared. They have their own processes that are perhaps not as fast as ours. So, when we're imagining a common baseline, it would be good to bring in broader traders and bankers so that we're all sharing the same data and not individually running the same checks."

08 Marcura

Unified Compliance

Compliance today does more than increase risk exposure. It slows down work and distracts teams from their core responsibilities.

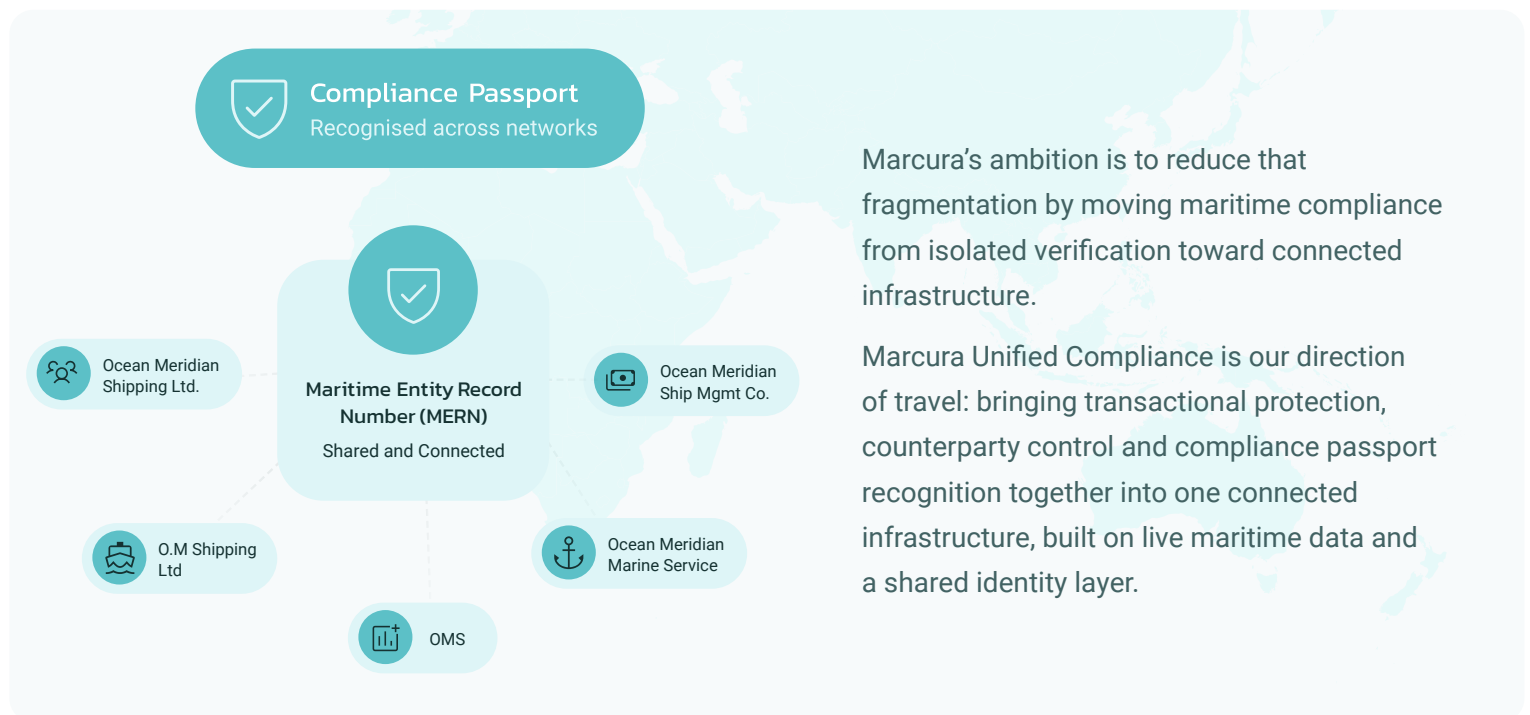
Operations managers chase documents. Finance teams pause payments for manual verification. Commercial teams wait for counterparty clearance. Compliance professionals spend time proving checks were performed instead of focusing on material risk.

Today, the same counterparty is screened repeatedly across organisations. Ownership structures are analysed multiple times. Documents are requested again and again.

The same work is duplicated across organisations, with no mechanism for recognition beyond internal controls.

Therefore, the problem is not only about regulatory complexity. It is fragmentation, of both data and policy.

Data sits in silos across platforms that do not speak to one another. Policy diverges across jurisdictions and across organisations, even when reviewing the same counterparty. The result is repeated verification, inconsistent outcomes and operational drag.



The data advantage

Compliance infrastructure only works when it is grounded in real maritime activity.

Marcura's platforms sit inside the industry's operational backbone.

For more than two decades, DA-Desk, ShipServ and MarTrust have processed millions of port calls, Statements of Facts, disbursement accounts, invoices, and billions in maritime payments. That means our compliance intelligence is built on live transaction data, not static registries or isolated database extracts.

That context matters because sanctions exposure does not reveal itself through a company name alone. It hides in ownership chains, related entities, vessel histories and behavioural patterns across transactions. Those connections become visible only where activity actually flows.

By operating at the point of transaction, Marcura is positioned to build compliance infrastructure backed by real relationships and evolving activity, rather than detached records.



100M+ Observed Relationships

KYCC - Know Your Counterparty's Counterparties

Dynamic



9M+ Transactions

KYT - Know Your Transaction

Operational



2M+ Legal Entities
(Trading and Non-Trading)

KYC - Know Your Counterparty

Persistent



300K+ Maritime Counterparties
(Trading)

KYD - Know Your Data

Master Layer

Three tiers of engagement

Organisations engage at the level matching their operational reality, risk appetite and internal capability.

Embedded Transaction Protection

Compliance must function where decisions are made.

Every agent nomination, supplier onboarding, counterparty engagement and payment instruction triggers automated screening inside operational workflows. Sanctions monitoring runs continuously.

Bank account changes are independently verified before funds move.

Protection runs in the background while operations continue at speed.

This is not an additional control layer. It is compliance by design.

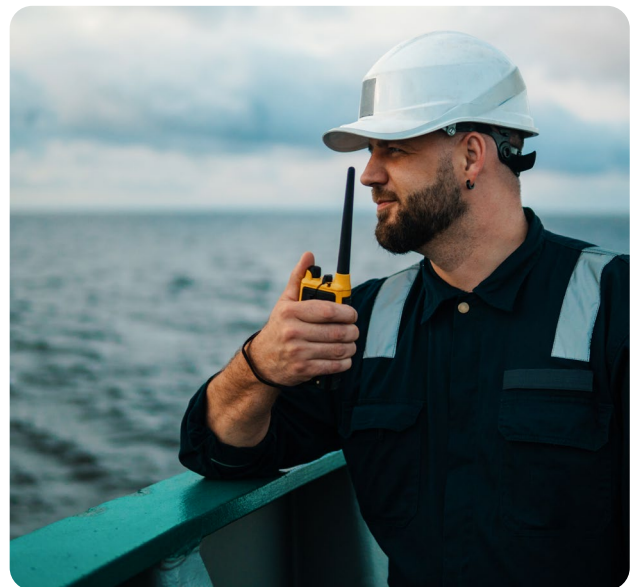


Counterparty Control

Embedded protection is the foundation. Control extends that foundation across your entire counterparty universe.

Counterparty Control covers operational and commercial counterparties, including owners, charterers, brokers, agents and vendors. Structured onboarding, deep ownership analysis and policy-aligned risk scoring provide visibility across your full portfolio.

This protects you from indirectly sanctioned counterparties or high-risk vessels using complex ownership structures or high-risk activities, reducing exposure to frozen payments, enforcement action, banking restrictions and reputational damage.



Control reduces risk. It also improves audit defensibility and decision confidence across departments.

But control alone does not eliminate duplication.

The Compliance Passport

The Compliance Passport is designed to move beyond isolated verification toward recognised compliance.

Counterparties can be verified once and recognised across participating organisations.

The model is powered by MERN™, the [Maritime Entity Record Number](#) that links entities, ownership structures and transaction history across systems. Consistent identity enables consistent recognition.

Screening outcomes are independently verified and shared across authorised network participants. Sensitive ownership details remain holder-controlled and anonymised when not disclosed.

Recognition does not require full disclosure. Ownership documentation, UBO records and corporate control structures remain under the control of the passport holder. The holder determines who may access detailed documentation, while verified screening outcomes remain visible across the authorised network. Verification cannot be influenced by selective disclosure.

There is no single global standard when it comes to risk acceptance. The infrastructure supports divergent regulatory regimes. Each participant applies its own policy but within a shared framework.



Verified once. Recognised across the network.

The impact is practical:

- ✓ Reduced duplicated due diligence
- ✓ Faster onboarding
- ✓ Lower compliance cost per counterparty
- ✓ Stronger bank and partner confidence
- ✓ Protection of long-term commercial relationships

One Infrastructure. Three Tiers. Complete coverage.

Choose the right level of compliance protection for your organisation

Transaction Protection

EMBEDDED

Included with DA-Desk, ShipServ and MarTrust

- ⦿ Automatic screening against OFAC, EU, UK, and UN sanctions lists
- ⦿ Embedded directly in product workflows
- ⦿ Continuous sanctions monitoring with alerts

Counterparty Coverage

Port Agents Suppliers
Vendors

Value

Protects your operational payments and port activity without slowing execution. Automatic sanctions screening and bank verification reduce fraud, payment errors, and last-minute disruptions.

Counterparty Control

ENHANCED

Extend protection beyond single transactions

- ⦿ Structured KYB verification and digital onboarding workflows
- ⦿ Deep ownership analysis and UBO mapping
- ⦿ Risk scoring aligned to your policy framework, covering other watchlists, PEPs or adverse media
- ⦿ Bank account verification and change control
- ⦿ Portfolio-level visibility across counterparties

Counterparty Coverage

Charterers Owners Operators
Brokers Agents Vendors
Shippers Receivers
Any other counterparty

Value

Provides you with control over all operational and commercial counterparties. Protects you against indirectly sanctioned counterparties or high-risk vessels, reducing frozen payments, enforcement exposure and reputational damage.

Compliance Passport

PRO

Move from isolated checks to shared intelligence

- ⦿ Verified once, recognised across the network
- ⦿ Powered by MERN™, the maritime entity identifier
- ⦿ Risk outcomes shared network-wide
- ⦿ Sensitive ownership details remain holder-controlled and anonymised when not disclosed
- ⦿ Shared infrastructure: your jurisdictions, your policy

Counterparty Coverage

Charterers Owners Operators
Brokers Agents Vendors
Shippers Receivers
Any other counterparty

Value

Gives you centralised control over counterparty risk across your entire portfolio, reducing compliance costs, safeguarding banking relationships and protecting long-term revenue.



The path from here

What transforms these capabilities into a network is shared verification that travels. Counterparties passing due diligence once, that result recognised by everyone who subscribes to the same standards.

The vision is clear. So are the obstacles. Regulatory frameworks govern what decisions one entity can rely on from another. Data standards must ensure verification performed in one context meets requirements in another. Policies need alignment tight enough that "approved" means the same thing everywhere. These aren't trivial issues and require a considered approach.

The economic logic, however, is hard to argue with. The current model is pure waste. Every organisation maintaining parallel verification infrastructure, the same counterparty vetted dozens of times. That's simply time, money, effort, all duplicated without adding protection.

The architectural foundation is in place. Early adopters are proving the model. The direction is set: from fragmented verification to connected assurance, from duplicated effort to collective intelligence, from compliance as bottleneck to compliance by design.

This guide was developed by Marcura,
whose compliance solutions serve
maritime organisations globally:

DA-Desk 

Port operations and
disbursement management

ShipServ 

Maritime procurement
and supplier networks

MarTrust 

Maritime payments
and crew payroll

The insights reflect Marcura's work with
maritime organisations managing compliance across
chartering, operations, procurement, and payments.

For questions about implementing these frameworks visit:

[Marcura.com/compliance](https://marcura.com/compliance)

