Shipping M&A with AI Assets

Diligencing Data Rights, Cybersecurity and the Safety Case

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Shipping acquisitions increasingly include artificial-intelligence models, operational data, connected equipment, remote-operations capability and safety evidence that may be central to fleet economics. The buyer can acquire shares or vessels while discovering later that critical data cannot be reused, supplier licences cannot be assigned, model performance does not transfer across the fleet, cyber controls are incomplete, or the safety case requires material rework. This paper develops an evidence-led diligence and integration framework for shipping transactions involving AI assets. It connects the International Maritime Organization's 2026 non-mandatory MASS Code, SOLAS, the International Safety Management Code and revised maritime cyber-risk guidance with IACS cyber-resilience requirements, data and intellectual-property rights, model validation, class and flag evidence, commercial contracts, insurance, financing and valuation. Forty modules cover the transaction perimeter, AI asset register, ownership and control, regulatory roadmap, safety functions, data provenance and rights, model and software dependencies, remote operations, human accountability, assurance, operational design domain, cyber architecture, incidents and recovery, contracts, carve-outs, fleet integration, capex, covenants, transaction protection and the first one hundred days. Five figures, five tables, eight frequently asked questions and twenty-six authoritative references support vessel-, system-, jurisdiction-, contract- and period-specific review. Illustrative methods and values require replacement with approved technical, regulatory, contractual and financial evidence. The framework does not substitute for maritime, flag, class, safety, cyber, data-protection, intellectual-property, competition, sanctions, legal, tax, accounting, valuation, insurance or investment advice.

JEL Classification: G34, L91, O32, O33, K24

Keywords: shipping M&A, maritime artificial intelligence, data rights, cybersecurity, safety case, autonomous ships, operational technology, due diligence, fleet integration, transaction value

1. Define the transaction and approval perimeter

State whether the deal is a share acquisition, vessel or fleet purchase, technology acquisition, joint venture, carve-out or merger. Freeze jurisdictions, flags, classes, vessels, shore entities, systems, contracts, people and closing conditions.

Controlled evidence includes transaction structure; perimeter; jurisdictions; flags; classes; asset list; closing condition. The immediate decision is to freeze what the buyer expects to own, operate and approve at completion. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

2. Build the AI asset register

Record each model, dataset, application, sensor, edge device, communications link, control interface, remote-operations component, documentation set and responsible team.

Controlled evidence includes asset identifier; purpose; owner; location; version; dependency; criticality; evidence. The immediate decision is to make the acquired AI operating system visible before value is assigned. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

3. Map ownership, possession and control

Legal ownership, physical possession, administrative access, operational authority and economic benefit may sit with different parties.

Controlled evidence includes legal title; licence; custody; access right; decision authority; beneficiary; restriction. The immediate decision is to separate control of an asset from permission to use or transfer it. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

4. Apply the regulatory baseline and roadmap

The 2026 non-mandatory MASS Code supports experience building while existing mandatory instruments continue to apply. The expected pathway towards mandatory rules affects design and integration choices.

Controlled evidence includes applicable convention; code; flag instruction; class rule; approval; effective date; roadmap. The immediate decision is to price current compliance and credible future adaptation separately. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

5. Map safety-critical functions

Navigation, propulsion, steering, power, communications, fire protection, watertight integrity, cargo, connectivity and remote-operation functions require clear safety boundaries.

Controlled evidence includes function; hazard; system; human role; fallback; verification; approval. The immediate decision is to connect every AI dependency to the ship function and failure consequence. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

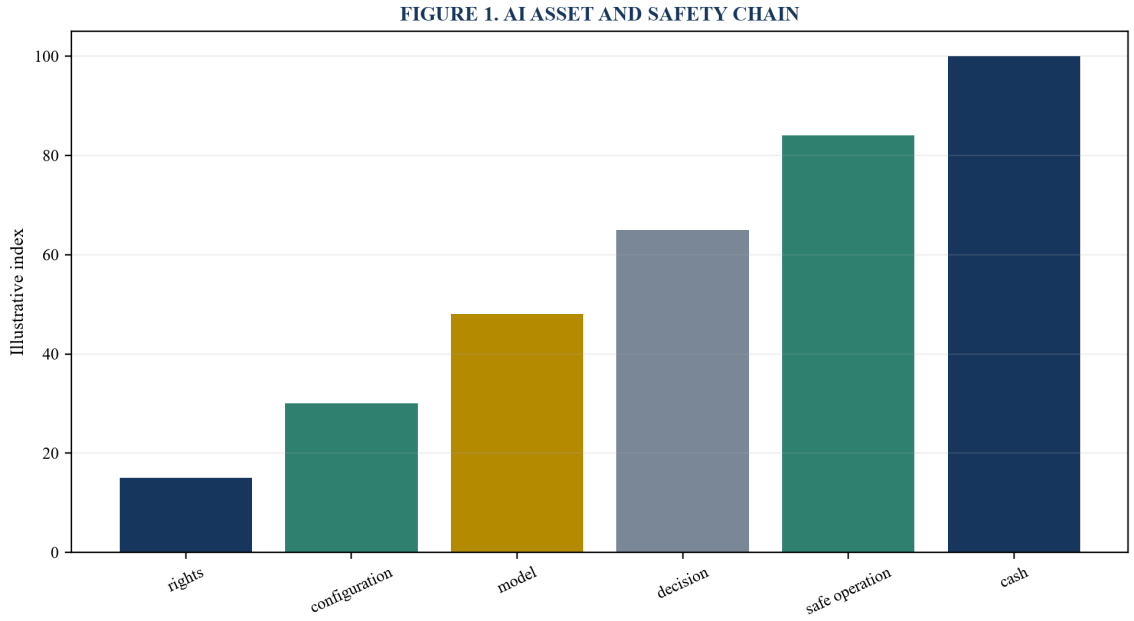
The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

Table 1. AI safety-function map

Function	Required evidence	Failure consequence
navigation	approved sensors, model and fallback	collision or grounding
propulsion and steering	control boundary and local recovery	loss of manoeuvrability
connectivity	coverage, priority and degraded mode	loss of remote capability
remote operations	authority, competence and handover	unsafe or ambiguous control

Replace illustrative classifications with company-specific evidence and approved transaction treatment.

Figure 1. AI asset and safety chain



The acquired asset extends from rights and configuration to human authority, operation and cash.

6. Trace operational-data provenance

Vessel data can originate from owner systems, yards, equipment makers, crew, charterers, ports, weather services and public authorities.

Controlled evidence includes source; collection authority; timestamp; transformation; quality; lineage; retention. The immediate decision is to show which evidence can support operations, training, diligence and claims. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

7. Diligence data rights and permitted use

Access to data does not establish ownership or unrestricted reuse. Contract, privacy, database, confidentiality and sector rules may constrain processing and transfer.

Controlled evidence includes rightsholder; licence; purpose; territory; term; transfer; deletion; audit. The immediate decision is to prove that post-closing use matches the acquired right. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and

outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

8. Protect crew and personal data

Crew, passenger, health, location, communications and performance information can carry distinct legal purposes and sensitivities.

Controlled evidence includes data category; lawful basis; notice; purpose; access; transfer; retention; deletion. The immediate decision is to preserve legitimate operations while limiting unlawful or excessive use. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

9. Test training-data legality and fitness

Training data should be lawfully obtained, representative of the intended operation, versioned and linked to exclusions and known limitations.

Controlled evidence includes dataset; right; population; exclusion; label; bias test; version; reviewer. The immediate decision is to avoid acquiring a model whose evidence cannot be reproduced or reused. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

10. Inventory models and decision authority

Catalogue models, rules, optimisation engines and embedded algorithms, including the decision they inform and the person or system authorised to act.

Controlled evidence includes model identifier; objective; input; output; threshold; approver; override; log. The immediate decision is to distinguish advice, automation and control within the operating model. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

11. Establish software and algorithmic IP

Source code, object code, model weights, configuration, documentation, inventions and know-how may have different owners and protection routes.

Controlled evidence includes creator; employer; assignment; repository; registration; trade-secret control; dispute. The immediate decision is to confirm ownership and practical access to maintain the acquired capability. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

12. Review open-source and third-party components

Software bills of materials should reveal licences, obligations, vulnerabilities and embedded components that affect distribution, modification and support.

Controlled evidence includes component; version; licence; notice; source obligation; vulnerability; maintainer. The immediate decision is to identify legal and operational dependencies before closing. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

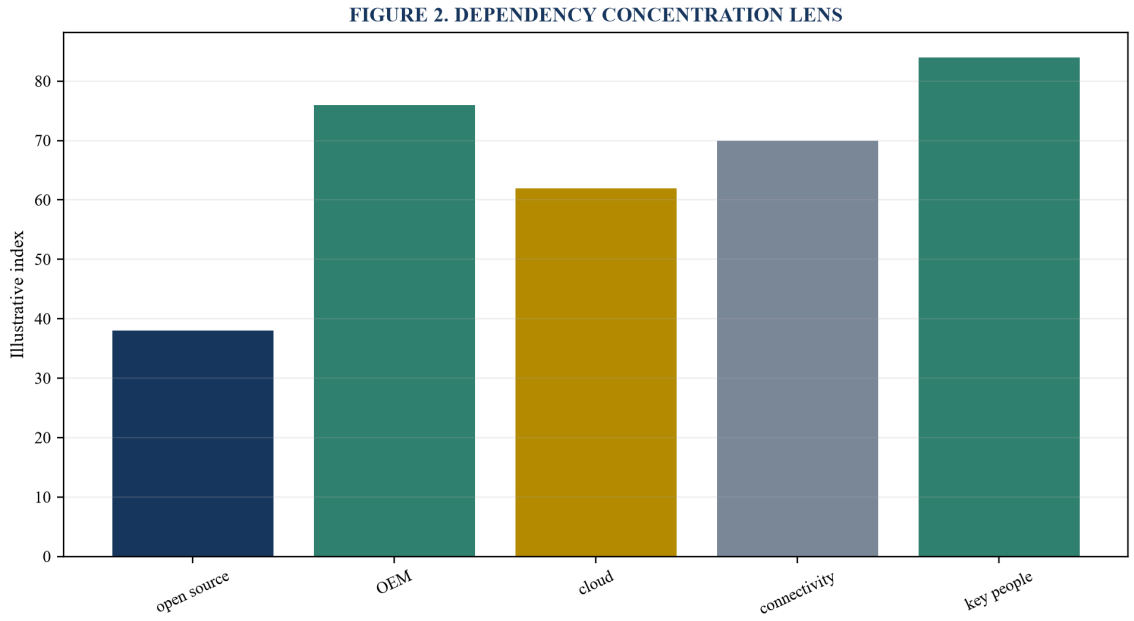
Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

Table 2. Software dependency review

Layer	Evidence	Transaction risk
proprietary code	ownership and repository access	missing maintenance capability
open source	SBOM, licence and notices	unmet obligations
vendor component	assignable licence and support	termination or hold-up
cloud and data service	portability and exit test	operational discontinuity

Replace illustrative classifications with company-specific evidence and approved transaction treatment.

Figure 2. Dependency concentration lens



Replace illustrative indices with target-specific contractual and technical evidence.

13. Map vendor and cloud dependency

AI capability may depend on cloud services, satellite links, chart providers, equipment OEMs, application vendors and proprietary interfaces.

Controlled evidence includes supplier; service; SLA; data location; subcontractor; termination; portability; cost. The immediate decision is to test whether the operating stack survives ownership change and supplier stress. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

14. Freeze hardware, software and configuration baselines

Performance and safety evidence should identify the exact sensor, compute, network, firmware, software, model and parameter configuration tested.

Controlled evidence includes configuration item; version; installation; calibration; change log; approval; rollback. The immediate decision is to prevent assurance evidence from being applied to a different system state. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

15. Diligence remote-operations capability

Remote Operations Centres require approved functions, communications resilience, situational awareness, competence, workload control and contingency arrangements.

Controlled evidence includes ROC location; function; staffing; connection; latency; fallback; exercise; approval. The immediate decision is to establish which remote capability transfers and remains operable. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

16. Test connectivity and service continuity

AI-enabled operations may depend on satellite, terrestrial, port and onboard networks with different coverage, latency, capacity and failure modes.

Controlled evidence includes link; provider; coverage; latency; redundancy; priority; outage record; fallback. The immediate decision is to model degraded and disconnected operation rather than continuous connectivity. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

17. Preserve accountable human roles

The master, crew, remote operators, designated person, engineers, vendor staff and management retain defined responsibilities despite automation.

Controlled evidence includes role; competence; authority; handover; escalation; override; fatigue; record. The immediate decision is to keep human responsibility explicit through closing and integration. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

18. Reconstruct the safety case

A safety case should connect intended operation, hazards, controls, verification, residual risk, competence and approval through a traceable argument.

Controlled evidence includes claim; hazard; control; evidence; assumption; owner; approval; limitation. The immediate decision is to test whether the assurance argument remains valid under buyer ownership. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

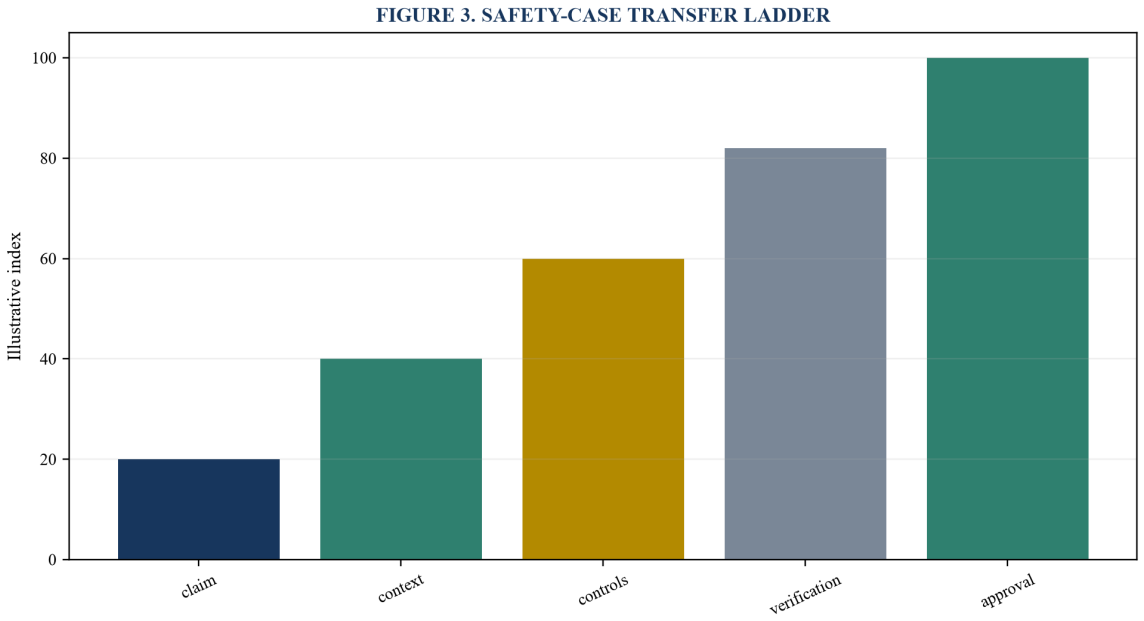
Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

Table 3. Safety-case transfer test

Layer	Evidence	Buyer question
claim	defined safe outcome	what is asserted?
context	operating domain and configuration	where does it apply?
control	technical and human barrier	what prevents harm?
proof	test, trial, survey and record	is it reproducible?
change	ownership and integration impact	what requires revalidation?

Replace illustrative classifications with company-specific evidence and approved transaction treatment.

Figure 3. Safety-case transfer ladder



Each transaction change should be tested against the claim, context, controls and proof.

19. Validate models and integrated performance

Model metrics should match the decision horizon and consequence. System validation should include integration, edge cases, degraded modes and human interaction.

Controlled evidence includes objective; test set; horizon; error; scenario; acceptance; reviewer; limitation. The immediate decision is to approve each model only for a defined operating decision and configuration. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

20. Define the operational design domain

State vessel types, routes, waters, weather, traffic, connectivity, port conditions, crew and remote support within which the capability is evidenced.

Controlled evidence includes geography; environment; traffic; vessel; equipment; connectivity; people; exclusion. The immediate decision is to avoid extrapolating trial evidence beyond the approved operating domain. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

21. Verify flag, class and statutory evidence

Certificates, class notations, approvals, exemptions, conditions, survey records and open recommendations should be reconciled to each vessel and system state.

Controlled evidence includes vessel; flag; class; certificate; notation; condition; survey; expiry. The immediate decision is to identify approvals that require renewal, transfer, revalidation or remediation. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

22. Build the cyber asset and trust-boundary map

Map vessel IT and OT, shore systems, remote access, suppliers, identities, data flows, safety interfaces and external connections.

Controlled evidence includes asset; zone; conduit; identity; privilege; protocol; owner; monitoring. The immediate decision is to connect cyber exposure to operational and safety consequence. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

23. Test IACS cyber-resilience applicability

IACS UR E26 addresses ship-level cyber resilience and UR E27 addresses onboard systems and equipment, subject to their applicability and class implementation.

Controlled evidence includes contract date; vessel scope; class rule; system scope; requirement; evidence; gap. The immediate decision is to separate mandatory applicability from useful diligence benchmarks. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

24. Review vulnerabilities and secure development

Diligence should cover threat modelling, secure design, code review, testing, vulnerability disclosure, patching and unsupported components.

Controlled evidence includes threat; weakness; component; severity; exploitability; patch; exception; owner. The immediate decision is to quantify residual exposure and the work required to maintain security. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or

persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

25. Reconcile cyber incidents and operational impact

Incident records should connect detection, containment, affected systems, vessel consequence, reporting, recovery, cost and lessons learned.

Controlled evidence includes incident; timestamp; system; impact; response; notification; cost; closure. The immediate decision is to test history against logs, insurer records and corrective action. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

26. Test resilience, recovery and manual fallback

Backups, spare equipment, alternative communications, local control, exercises and recovery objectives should support safe continuity.

Controlled evidence includes failure mode; fallback; recovery objective; backup; exercise; result; dependency. The immediate decision is to prove recovery for safety-critical and cash-critical services. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

27. Assess insurance, liability and casualty evidence

AI does not displace contractual, statutory or tort responsibilities. Coverage, exclusions, disclosure and causation require transaction-specific review.

Controlled evidence includes policy; insured; limit; exclusion; notification; claim; warranty; subrogation. The immediate decision is to identify retained risk and change-of-control implications. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

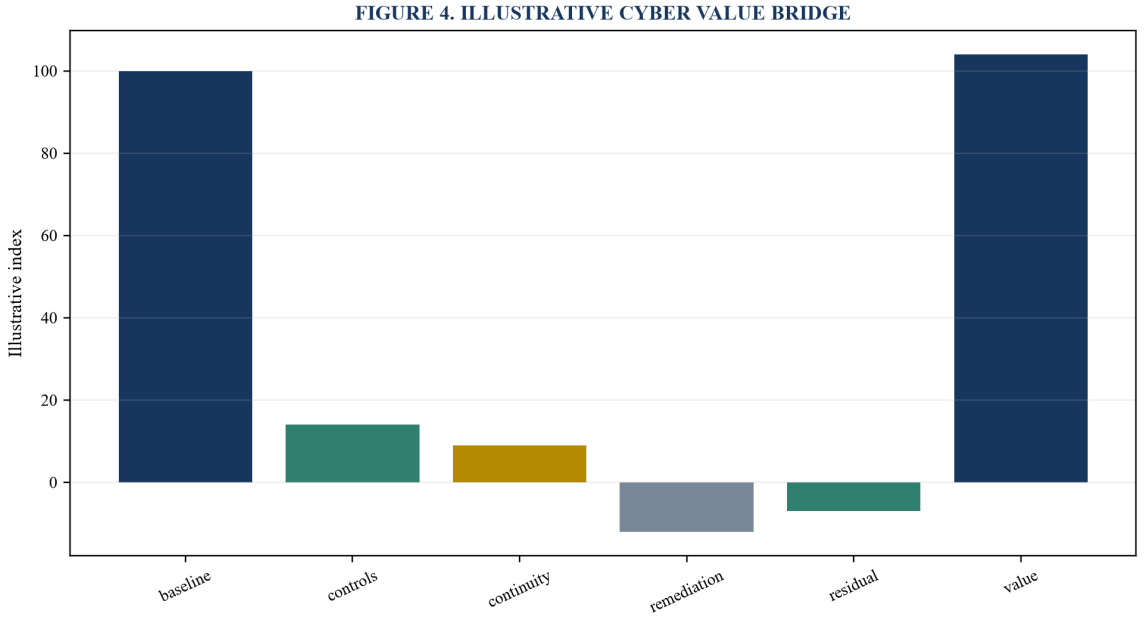
The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

Table 4. Cyber-to-value bridge

Exposure	Evidence	Financial channel
vessel outage	incident and recovery records	off-hire and repair
data compromise	scope and notification	response and liability
supplier access	privilege and contract	continuity and remediation
safety consequence	hazard and control failure	casualty and insurance
remediation	approved work programme	capex and downtime

Replace illustrative classifications with company-specific evidence and approved transaction treatment.

Figure 4. Illustrative cyber value bridge



Residual cyber exposure and remediation should be reconciled after full cost.

28. Review technology contracts for change of control

Licences, support, hosting, connectivity, data, maintenance and development agreements may contain assignment, consent, termination and price-reset rights.

Controlled evidence includes contract; counterparty; service; assignment; consent; termination; remedy; transition. The immediate decision is to secure continuity and evidence through completion. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

29. Diligence charter and customer commitments

Performance promises, data-sharing terms, route obligations, service levels and liability allocation can determine whether AI benefits convert into cash.

Controlled evidence includes charter; customer; commitment; data right; KPI; credit; claim; renewal. The immediate decision is to reconcile the technical proposition to enforceable commercial economics. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

30. Concentrate critical supplier risk

A small supplier, key engineer or proprietary component can control fleet availability and integration timing.

Controlled evidence includes supplier; component; spend; substitutability; lead time; inventory; financial health; exit. The immediate decision is to expose single points of operational and bargaining failure. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

31. Design carve-out and transition services

A seller may host repositories, identities, connectivity, data lakes, service desks or ROC functions that the target cannot operate independently on day one.

Controlled evidence includes shared service; owner; dependency; TSA; duration; milestone; exit test; cost. The immediate decision is to fund and govern a credible path to standalone operation. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

32. Plan fleet and enterprise integration

Integration should sequence safety authority, configuration, networks, identity, data, model validation, crew, ROC, suppliers and finance without creating mixed-control states.

Controlled evidence includes fleet cohort; target state; dependency; migration; test; approval; rollback; owner. The immediate decision is to integrate by evidence-gated vessel cohorts. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

33. Build the transaction value bridge

Separate current evidenced cash, funded improvement, required remediation, integration benefit, buyer-specific synergy and terminal-value assumption.

Controlled evidence includes baseline cash; benefit; timing; capex; opex; tax; risk; attribution. The immediate decision is to recognise recurring and transferable value once. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

34. Control synergy claims and double counting

Fuel, off-hire, crewing, insurance, maintenance, safety and commercial benefits can overlap or depend on the same intervention.

Controlled evidence includes synergy; mechanism; baseline; dependency; overlap; cost; owner; period. The immediate decision is to retain one causal route from capability to cash. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

35. Estimate compliance and integration capex

Include hardware, software, connectivity, class, flag, trials, cyber remediation, data work, people, shore facilities and contingency.

Controlled evidence includes work package; quantity; unit cost; schedule; dependency; contingency; approval. The immediate decision is to price the complete cash requirement and downtime consequence. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow

it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

36. Translate findings into debt and covenant terms

Lenders may focus on asset availability, cash volatility, capex, insurance, class, cyber incidents, concentration and permitted technology change.

Controlled evidence includes facility; borrower; collateral; covenant; information right; event; cure; reserve. The immediate decision is to connect technical diligence to repayment protection. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

37. Allocate risk in transaction documents

Representations, warranties, covenants, conditions, indemnities, escrows, price adjustment and insurance should address evidenced risks without replacing diligence.

Controlled evidence includes risk; knowledge; disclosure; remedy; cap; survival; escrow; condition. The immediate decision is to match contractual protection to severity, control and recoverability. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Evidence should remain vessel-, system-, configuration-, jurisdiction-, contract- and period-specific. The review should preserve failed tests, overrides, incidents, open conditions and adverse operating outcomes.

The operating team and finance team should use the same definitions. Native records should support aggregate dashboards, and sample testing should follow representative cases from input through outcome and cash. Exceptions, failed cases and client concessions remain part of the population. Reconciliation should cover opening and closing balances, acquisitions, disposals, foreign exchange, allocation changes and manual adjustments that could otherwise mimic operating improvement.

38. Execute the first one hundred days

Sequence access, authority, incident readiness, key-person retention, supplier consents, safety and cyber baselines, controlled migrations, cash tracking and board reporting.

Controlled evidence includes day-one control; milestone; owner; dependency; evidence gate; budget; escalation. The immediate decision is to stabilise acquired operations before scaling

integration. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Finance should distinguish current operation, required remediation, funded integration, forecast improvement and buyer-specific synergy. Every benefit needs timing, full cost, responsibility and a route to cash.

Decision makers need both upside and downside. The analysis should state which party controls conversion, what investment remains, when cash appears, which risks survive and whether the result continues after a change of ownership. Unsupported precision should be replaced with bounded scenarios. The committee should record the decision consequence of each range, including price, structure, funding, covenant, integration and monitoring implications.

39. Build the transaction evidence room

Index native technical, regulatory, contractual, cyber, operational and financial records with owners, periods, versions and unresolved findings.

Controlled evidence includes document; source; owner; vessel; system; period; version; finding. The immediate decision is to make every material conclusion independently traceable. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Technical, legal, safety, cyber, operational and finance teams should use stable identifiers and cut-offs. Representative evidence should be traced from source record through decision and outcome.

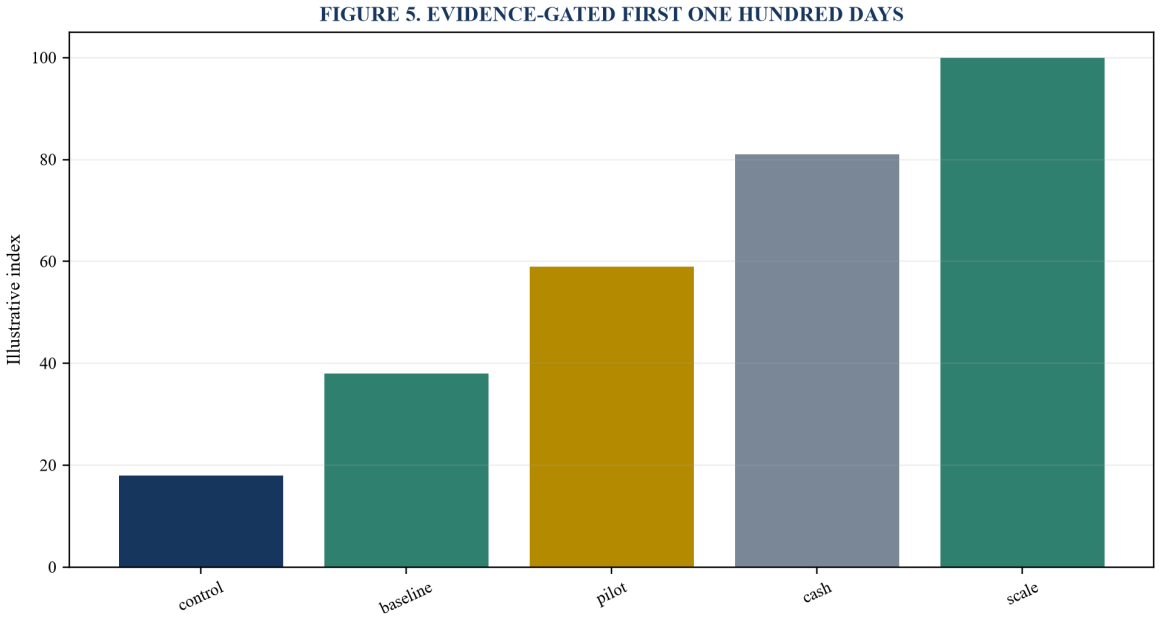
The analytical unit should remain stable from source record to valuation conclusion. Reviewers should see the population, exclusions, period, owner and reconciliation to finance. Where evidence is incomplete, the model should retain a range and identify the action needed to narrow it. Comparisons should preserve product, customer, site, complexity and market conditions; aggregation should not conceal adverse cohorts or delayed consequences.

Table 5. Evidence-gated integration

Period	Primary work	Gate
days 1-30	control, access, incidents and consents	approve stabilisation
days 31-60	baselines, validation and pilot cohort	approve controlled migration
days 61-100	cash bridge, remediation and governance	approve scaled integration

Replace illustrative classifications with company-specific evidence and approved transaction treatment.

Figure 5. Evidence-gated first one hundred days



Integration should follow safety, cyber, operational and cash proof.

40. Conclusion

Shipping M&A with AI assets creates defensible value when rights, safety, cyber resilience, operating performance and cash remain valid after ownership and fleet integration.

Controlled evidence includes asset register; right; configuration; safety case; cyber control; contract; cash; owner. The immediate decision is to use one evidence chain from acquired capability to post-closing value. Definitions should remain stable across transaction, technical, regulatory, operational and financial records.

Decision makers need bounded downside for missing rights, unsupported software, model error, unsafe integration, cyber incident, approval delay, supplier failure and weak adoption.

Evidence should distinguish observation, estimate, management plan and transaction judgement. A supported claim includes timing, full cost, dependency, transferability and a cash consequence. Sensitivity should show how the conclusion changes when adoption, demand, quality or persistence underperforms. Material assumptions need validation dates, accountable owners and explicit expiry conditions so that stale expectations do not survive into pricing or financing decisions.

References

[1] International Maritime Organization, IMO adopts first global Code for autonomous ships, https://www.imo.org/en/mediacentre/pressbriefings/pages/imo-adopts-mass-code.aspx

[2] International Maritime Organization, International Code of Safety for Maritime Autonomous Surface Ships, https://www.imo.org/en/mediacentre/pressbriefings/pages/imo-adopts-mass-code.aspx

[3] International Maritime Organization, Interim Guidelines for MASS Trials, MSC.1/Circ.1604, https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/MSC.1-Circ.1604%20-%20Interim%20Guidelines%20For%20Mass%20Trials%20(Secretariat).pdf

[4] International Maritime Organization, International Convention for the Safety of Life at Sea, https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx

[5] International Maritime Organization, International Safety Management Code, https://www.imo.org/en/ourwork/humanelement/pages/ismcode.aspx

[6] International Maritime Organization, Maritime Cyber Risk, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

[7] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.3, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf

[8] International Maritime Organization, Maritime Cyber Risk Management in Safety Management Systems, MSC.428(98), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[9] International Association of Classification Societies, UR E26 Cyber Resilience of Ships, https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e26-new

[10] International Association of Classification Societies, UR E27 Cyber Resilience of On-Board Systems and Equipment, https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1

[11] International Association of Classification Societies, Recommendation 166 on Cyber Resilience, https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new

[12] International Organization for Standardization, ISO 23806:2022 Ships and Marine Technology Cyber Safety, https://www.iso.org/standard/77027.html

[13] International Organization for Standardization, ISO 19847 Shipboard Data Servers, https://www.iso.org/standard/71995.html

[14] International Organization for Standardization, ISO 19848 Standard Data for Shipboard Machinery and Equipment, https://www.iso.org/standard/77037.html

[15] National Institute of Standards and Technology, Cybersecurity Framework 2.0, https://www.nist.gov/cyberframework

[16] National Institute of Standards and Technology, Secure Software Development Framework, https://csrc.nist.gov/Projects/ssdf

[17] National Telecommunications and Information Administration, Software Bill of Materials, https://www.ntia.gov/page/software-bill-materials

[18] European Union, Regulation EU 2024/1689 Artificial Intelligence Act, https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[19] European Union, Regulation EU 2023/2854 Data Act, https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[20] European Union, Regulation EU 2016/679 General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[21] Organisation for Economic Co-operation and Development, OECD AI Principles, https://oecd.ai/en/ai-principles

[22] World Intellectual Property Organization, Intellectual Property and Artificial Intelligence, https://www.wipo.int/about-ip/en/frontier_technologies/ai_and_ip.html

[23] International Chamber of Shipping, Guidelines on Cyber Security Onboard Ships, https://www.ics-shipping.org/publication/guidelines-on-cyber-security-onboard-ships/

[24] International Valuation Standards Council, International Valuation Standards, https://ivsc.org/standards/

[25] IFRS Foundation, IFRS Accounting Standards, https://www.ifrs.org/issued-standards/list-of-standards/

[26] International Maritime Organization, Convention on the International Regulations for Preventing Collisions at Sea, https://www.imo.org/en/about/conventions/pages/colreg.aspx

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.