INDUSTRY USE CASE

Maritime & Yachting

Ship Operators, Commercial Vessels, Port Facilities & Yacht Management

"Port-ready. Flag-state compliant. Cyber-resilient at sea."

Maritime organizations face a rapidly evolving cybersecurity regulatory environment. The IMO's maritime cyber risk management guidelines are now incorporated into ISM Code compliance, and port state control inspections increasingly include cybersecurity components. Auditerra helps commercial vessel operators, port facilities, and yacht management companies achieve and maintain compliance with global maritime regulations — without disrupting operations.

SOLAS | MARPOL | ISM Code | STCW | ISPS Code | IEC 62443

The Challenge

- IMO Resolution MSC-FAL.1/Circ.3 requires cyber risk management to be integrated into SMS by 2021 — but many operators have not yet fully implemented or documented this integration.
- Port state control inspections by Paris MOU, Tokyo MOU, and USCG increasingly include cyber risk management verification as part of ISM Code assessments.
- SOLAS Chapter XI-2 and the ISPS Code require ship security plans and port facility security plans that must now address cyber vulnerabilities in navigation, communication, and cargo systems.
- Superyacht operators face a unique intersection of flag state requirements, MLC compliance, and owner privacy obligations that create a complex multi-framework environment.
- OT systems (ECDIS, AIS, GMDSS) are increasingly internet-connected and vulnerable — but most crew and shore-side staff lack cybersecurity training.

Compliance Frameworks We Cover

ISM Code (Cyber)

IMO requires cyber risk management to be incorporated into Safety Management Systems under the ISM Code. Documented cyber risk assessments and procedures are required for flag state and port state compliance.

SOLAS / ISPS Code

SOLAS Chapter XI-2 and the ISPS Code require ship and port facility security plans that increasingly must address cybersecurity vulnerabilities in safety-critical systems.

MARPOL

Environmental compliance documentation intersects with cybersecurity for vessels using electronic record books and automated reporting systems subject to flag state inspection.

STCW Cyber Training

Crew cyber awareness training aligned to STCW competency frameworks is increasingly required by flag states and recognized as a Port State Control deficiency area.

NIST CSF / IEC 62443

For port facilities and shore-based OT environments, NIST CSF and IEC 62443 (industrial control system security) provide the underlying technical framework for maritime cyber programs.

How Auditerra Engages — Our Process

Step 1 — Demo

A no-pressure, industry-tailored demo so you see exactly how our platform and auditors work together before any commitment.

Step 2 — Readiness Check

We conduct a gap assessment to map your current compliance posture, identify risk areas, and build a prioritized remediation roadmap.

Step 3 — Active Engagement

Our certified auditors don't hand you a to-do list. They work alongside your team — reviewing evidence, walking through controls, and personally resolving gaps in real time.

Step 4 — Continuous Monitoring

Compliance doesn't end at certification. Auditerra monitors your posture year-round, alerts you to drift, and keeps you audit-ready at all times — not just during audit season.

Why Not Big 5 or SaaS-Only?

Provider	What You Get	What's Missing
Big 5 Consulting	Deep expertise, global reach	Enterprise pricing — out of reach for most
SaaS-Only Platforms	Evidence collection platform	No human auditor — you're on your own
Auditerra	Platform + certified human auditors	Nothing. Custom pricing. Full engagement.

Flag State Inspection Readiness & OT Security at Sea

Maritime cybersecurity compliance is uniquely challenging because the threat surface spans operational technology (ECDIS, AIS, engine management), IT systems (crew communications, cargo management), and shore-based infrastructure — all under the oversight of flag states, port state control, and classification societies. Auditerra helps vessel operators document cyber risk management procedures within their SMS, prepare for flag state surveys and port state inspections, and implement crew training programs aligned to STCW competency requirements. For superyacht management companies, we build compliance programs that satisfy the flag state (Cayman, Marshall Islands, Malta) while addressing the owner's data privacy and operational security expectations.

What You Get with Auditerra

✓ ISM Code cyber risk management integration into existing SMS documentation

✓ Cyber risk assessment for vessel IT and OT systems (ECDIS, AIS, GMDSS, cargo systems)

✓ Ship Security Plan and Port Facility Security Plan cyber component development

✓ Flag state survey and port state control inspection readiness documentation

✓ Crew cyber awareness training program aligned to STCW competency frameworks

✓ Continuous monitoring of cyber posture for fleet operators and shore-based management teams

---

Ready to See It in Action?

Book your no-obligation demo at **auditerra.com/demo** or reach out directly at **compliance@auditerra.com**. We'll tailor the conversation to your industry, your frameworks, and your timeline — no generic pitch decks.