DRAKE
MARITIME SERVICES

MARITIME CYBER ANALYSIS

IMO 2026 Cyber Risk Requirements: What Operators Must Show

There is no new 2026 rule. The obligation has existed since 2021, and what changed is the need to prove a practice rather than hold a policy.

MARITIME CYBER DESK | REV. A · JUN 2026

The one thing worth getting straight before anything else is this: you have to be able to show cyber risk management, not just assert it. An inspector no longer accepts a policy document as proof. They want to see that cyber risk is identified, controlled, exercised, and recorded across your fleet, and that the people on board can explain their part in it. That shift, from holding a policy to proving a practice, is what "IMO 2026" really means for operators.

BOTTOM LINE UP FRONT

1. No new headline cyber rule arrived in 2026. The binding obligation has existed since 2021 under the ISM Code, and what has changed is the weight of scrutiny behind it.
2. The test is demonstration. An inspector wants to see cyber risk identified, controlled, exercised, and recorded across the fleet, with the crew able to explain their part.
3. The same documentation that satisfies an auditor protects a commercial position, because charterers, claims handlers, and insurers read it the same way.

It helps to clear up a common misunderstanding first. No new headline cyber rule arrived from the International Maritime Organization this year. The binding obligation has existed since 2021, and what has changed since is the weight of scrutiny behind it.

01 The short version of why

The foundation is Resolution MSC.428(98), which since 2021 has required cyber risk to be managed inside a company's Safety Management System under the ISM Code. The important distinction is that the placement of cyber in the SMS is mandatory and audited, while the detail of how you do it is yours to scale to the complexity of your ships. The guidance that describes good practice, circular MSC-FAL.1/Circ.3, is recommendatory, which operators sometimes misread as optional. The system being there is not optional. The shape of it is flexible.

That guidance was refreshed in April 2025 to its third revision, and the update matters. Rev.3 moved the guidance onto version 2.0 of the NIST Cybersecurity Framework, where it had previously referenced version 1.0. Two consequences follow for operators. First, governance is now explicit, which means senior

management ownership of cyber risk rather than treating it as an engine-room IT problem. Second, supplier accountability is now explicit. You are expected to verify that your external service providers and software vendors manage cyber risk appropriately, and to hold evidence that you checked. A general quality certificate from a vendor does not answer that question. A current information security certificate whose scope actually covers the software they build for you does.

A few other regimes apply depending on the ship and the trade, and operators are increasingly judged against the whole stack rather than the IMO floor alone. Classification societies enforce cyber resilience through IACS Unified Requirements E26 and E27, which apply to vessels contracted for construction on or after 1 July 2024, so they bite on newbuilds and on design and handover. The United States Coast Guard rule reaches vessels and facilities in US waters, and its one genuinely 2026 deadline is the personnel training requirement that took effect in mid-January 2026, with a designated cyber security officer and an approved plan due in 2027. In the European Union, the NIS2 Directive pulls shipping companies and ports into national cyber law. For tanker operators, the charterer dimension often bites hardest, since the OCIMF inspection and assessment regimes examine cyber security directly and a weak showing can cost business. A proposed Maritime Cyber Code points toward harmonising this patchwork over time, which rewards operators who build solid documentation now.

02 Who checks, and when

Cyber risk management is verified at the same ISM audits that confirm your Document of Compliance and your Safety Management Certificate. It is increasingly probed at port state control, and it shows up in charterer questionnaires before a fixture.

> **The same documentation an auditor wants is the documentation that protects a commercial position.**

The practical effect is that charterers, claims handlers, and insurers read it the same way.

03 What to show: a working checklist

This is the heart of it. Grouped under the five functional elements of the framework, here is the evidence that demonstrates a real system. Treated as a self-assessment, it also shows you where the gaps are.

Identify

- [ ] A documented cyber risk assessment for the company and its vessels, with a method behind it rather than a generic template.
- [ ] A maintained inventory of computer-based systems on board, covering operational technology (navigation, propulsion, steering, cargo handling) as well as ordinary IT.
- [ ] A map of remote access paths and vendor connections, with a network diagram pitched at a practical operational level.
- [ ] Records that you assessed the cyber posture of key suppliers and software vendors.

Protect

- [ ] Access control with individual accounts, least privilege, and records that leavers were removed.
- [ ] A patching and update routine for navigation and other critical software, with dates.
- [ ] A removable media policy and a basic onboard hygiene checklist.
- [ ] Controlled, approved, and logged vendor remote access.

Detect

- [ ] A defined way for anomalies to be noticed and reported by the crew.
- [ ] Whatever monitoring suits the ship's complexity, with evidence it is actually reviewed.

Respond

- [ ] An incident response procedure the crew can follow, with roles and an escalation chain, ship and shore, including named deputies.
- [ ] A record of the most recent drill.
- [ ] A log of any cyber incidents, which the guidance specifically expects you to keep.

Recover

- [ ] Backups of critical systems.
- [ ] Proof that a restore has actually been tested, with timestamps, rather than evidence that copies merely exist.

The thread running through all of it is traceability. An inspector should be able to follow any claim from policy to practice to record without a gap.

04 What this looks like in practice

Picture an ordinary mid-size operator with a thin cyber binder assembled a few years ago. It passed an early ISM audit because the auditor, new to cyber, checked that a document existed. The binder names a policy, references the IMO circular, and stops there.

The trouble surfaces later. A port state control officer asks the master to walk through what happens if the electronic chart system behaves strangely, and the master has not seen the procedure. A charterer's questionnaire asks for evidence that backups can be restored and for the security credentials of the planned maintenance software vendor. The operator has neither. The binder described a system that was never built on board, and the gap between the paper and the ship is now visible to exactly the people whose opinion carries commercial weight.

The fix is not exotic. The operator builds an honest asset inventory first, because almost everything else depends on knowing what is connected. It brings vendor remote access under control and gathers supplier certificates. It runs a restore test on one critical system and keeps the evidence. It assigns clear ownership ship and shore, runs a drill, and files the record. At the next audit the same auditor follows a claim from the policy to the crew to the log, and finds no gap. Nothing about that work is advanced. It is the basics, done and documented.

05 Where operators most often fall short

The failures that show up are remarkably consistent, and very few involve sophisticated attacks.

INVENTORY	The missing or unreliable asset inventory. An operator who cannot say what is connected cannot manage its risk.
ACCESS	Uncontrolled vendor remote access, often the single highest-risk pathway into a ship and the one least likely to be logged.
BACKUPS	Untested backups, where copies are made but recovery has never been proven.
OWNERSHIP	Unclear ownership, with cyber treated as someone else's job and no named person accountable.
OT	Operational technology neglected next to IT, despite being the part that affects steering, propulsion, and cargo.
SUPPLIERS	Supplier risk, as managers who never checked a vendor's credentials find that accountability has shifted to them.

TRAINING	Training that is paper-thin, present in the records but absent from the crew's ability to demonstrate a response in a drill.

06 What to do next

Start by confirming which regimes actually apply to your fleet and trade, since the IMO baseline, class requirements, flag and port-state rules, and charterer expectations each have a different scope. Then work the checklist in order of dependency. Build or refresh the asset inventory first. Bring vendor remote access under control and collect supplier certificates. Test a restore and keep the evidence. Assign ownership ship and shore, run a drill, and file the record. Close the loop by reviewing the whole arrangement against the five functional elements and fixing whatever surfaces. Done this way, cyber compliance stops being a scramble before each audit and becomes a steady, demonstrable part of how the fleet is run.

CLASSIFICATION	DESK	DATE	BASIS
ILLUSTRATIVE ANALYSIS SAMPLE	MARITIME CYBER DESK	REV. A · JUN 2026	IMO · IACS · USCG · EU