

Fleet cyber governance checklist

Fifteen questions to ask the teams and vendors. Answer for two ships of the same class; where the answers differ, that gap is usually the first governance finding.

Ship A

Ship B

INVENTORY AND OWNERSHIP

Is there an OT asset inventory for each ship, and who keeps it current?		
Who owns OT security on board: IT, the chief engineer, or the OEM?		
Which systems are safety critical, and are they on separate networks?		

CONNECTIVITY AND REMOTE ACCESS

How many satcom and LEO links does each ship have, and what can reach OT through them?		
Which vendors have remote access, how is it approved, and is it logged and time-limited?		
Is guest and crew traffic kept off the bridge and machinery networks?		

VENDORS, OEMS AND SHIPYARDS

Do contracts require IACS E27 or IEC 62443 security from suppliers?		
How do OEMs deliver and test patches, and who signs off on board?		
Do new builds and refits go through a cyber review before delivery?		

DETECTION AND RESPONSE

Can the team see OT network traffic at sea, or only IT?		
Does the incident response plan cover a ship at sea with limited bandwidth?		
When did the bridge, engine room, and shore teams last run a cyber tabletop together?		

COMPLIANCE AND REPORTING

Which vessels and U.S. terminals fall under the USCG rule, and are they on track for July 16, 2027?		
Is cyber risk in each ship's Safety Management System, as IMO expects?		
What does the board see each quarter, and does it show OT as well as IT?		