

# Italy's New Maritime Cybersecurity Rules

// CIRCULAR NO. 177/2025 // UPDATE OF SECURITY MEASURES REQUIREMENTS FOR NATIONAL VESSELS



## The Core Shift: Cyber is a mandatory safety measure, not an IT issue

Cyber protection must be embedded into SMS, procedures, and management oversight.

### Who Is Affected?

Italian-flag vessels and the shore-side organizations supporting them.

Systems covered include (examples):



#### Navigation

Bridge & Manoeuvring



#### Propulsion

Steering & Power



#### Operations

Passenger & Cargo



#### Connectivity

Ship/Shore Comms, Crew And Passenger connectivity



#### Resilience

Business Continuity

## What Companies Must Do



### Integrate Cyber into SMS

Embed cyber risk governance into Safety Management System (SMS) and ISM company policies, responsibilities, and emergency preparedness, in line with **IMO, IACS UR E26** and **NIS2** requirements.



### Assess Cyber Risk

Perform **risk assessment** for all critical systems, IT/OT interfaces, remote access, and vendor connections.



### Implement Controls

**Enforce** access control and authentication, network segregation, network controls, patching, malware defense, third-party security, crew training, and backup testing.

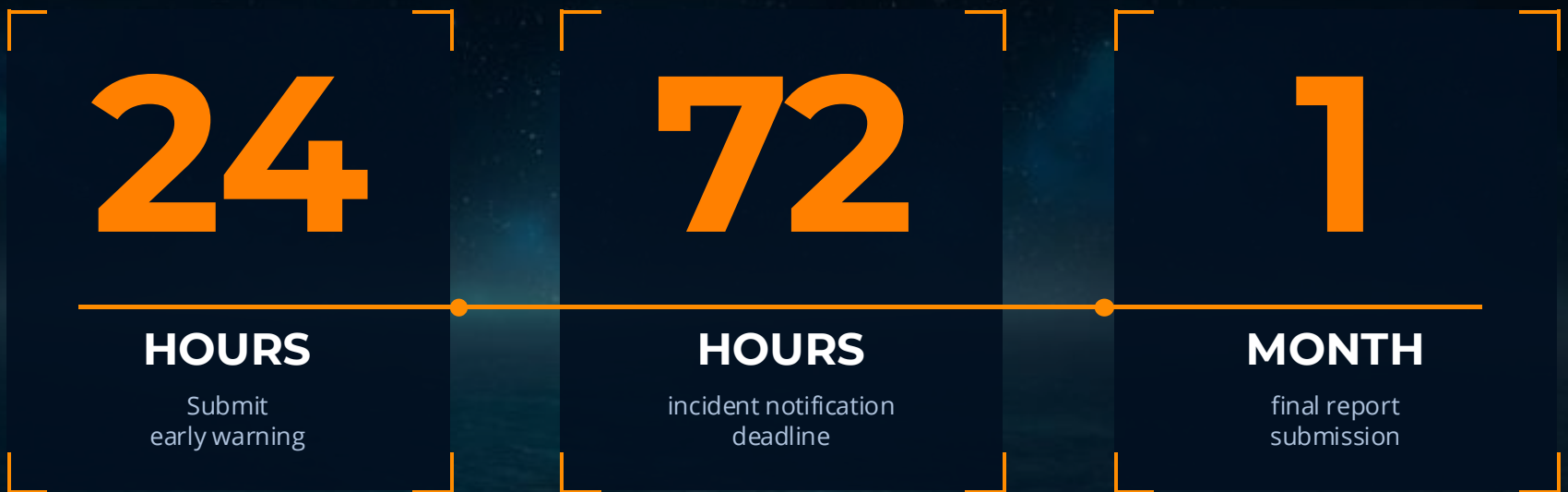


### Executive Takeaway

Cybersecurity is now part of safe navigation governance. Authorities expect documented controls, trained personnel, and management oversight.

# REQUIRED ACTION, RESPONSIBILITIES AND ACCOUNTABILITY

MANDATORY INCIDENT REPORTING TO NATIONAL CIRT, COAST GUARD AND IMRCC



## Responsibility of executives

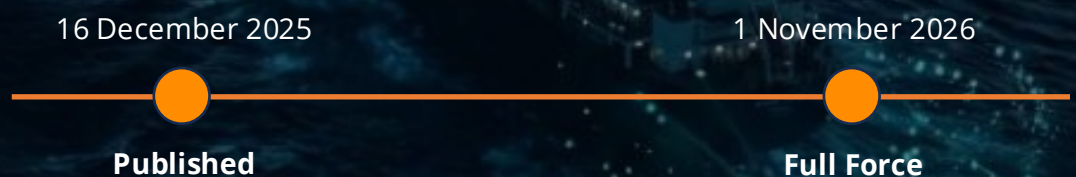
- Approve cybersecurity measures
- Oversee implementation
- Ensure sufficient budget resources and expertise
- Integrate cyber into safety governance
- Ensure serious incidents are escalated and reported
- Receive appropriate management-level training

*Cyber compliance cannot be left entirely to IT or external suppliers.*

### Why this matters

- Audit and inspection findings
- Corrective actions and greater regulatory scrutiny
- Exposure under Italy's cybersecurity framework
- Increased focus on management's personal oversight role

## Implementation Timeline



## Recommended next steps

- ✓ Confirm scope across ships, entities, and shore systems
- ✓ Appoint an executive owner and operational cyber lead
- ✓ Complete a cyber risk and compliance gap review
- ✓ Review vendor and third-party access arrangements
- ✓ Prioritize fixes for remote access, backups, and segregation
- ✓ Put cyber compliance on the board agenda

**Bottom line: For shipping companies, cybersecurity is now a safety, compliance, and leadership strategy.**