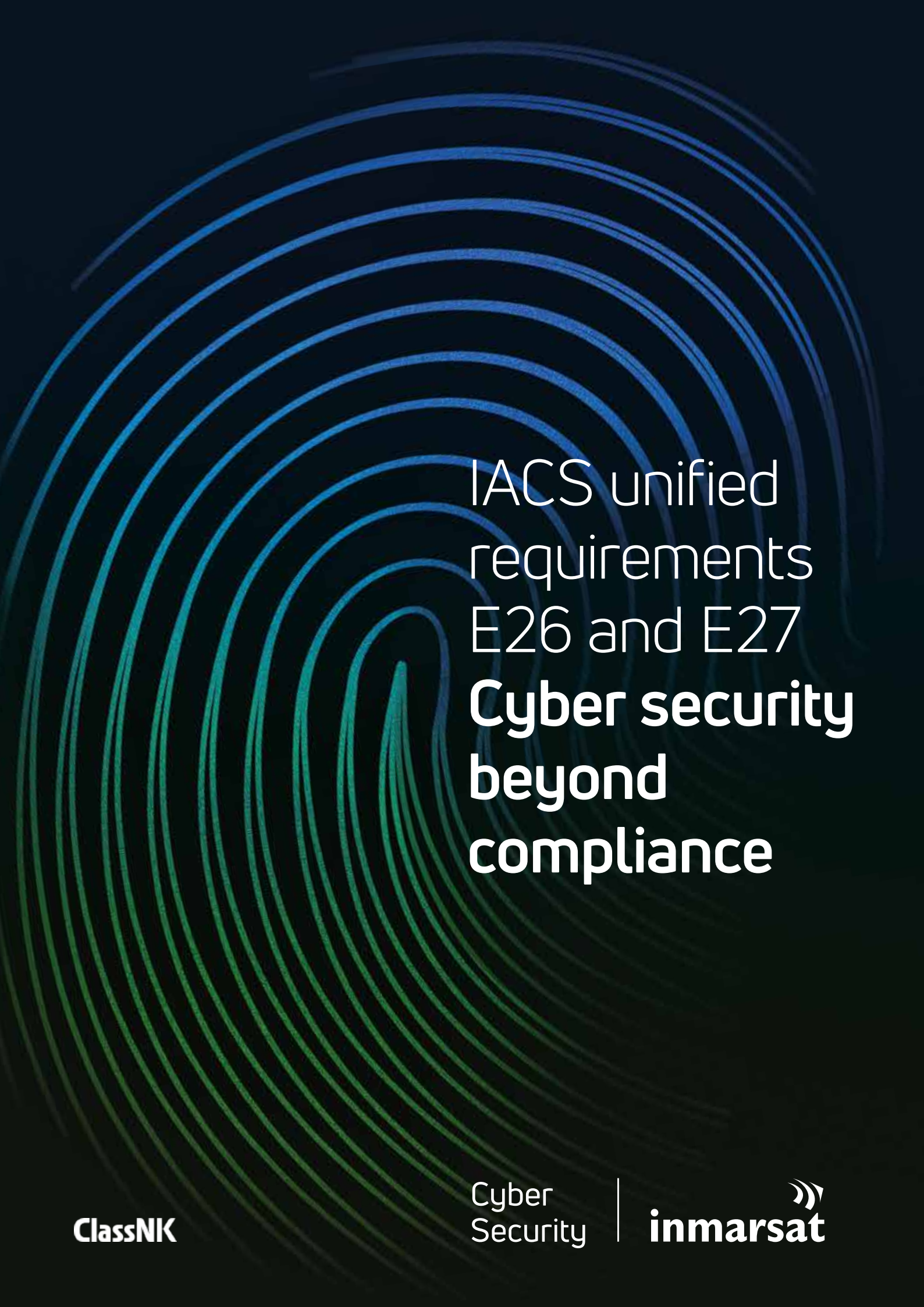
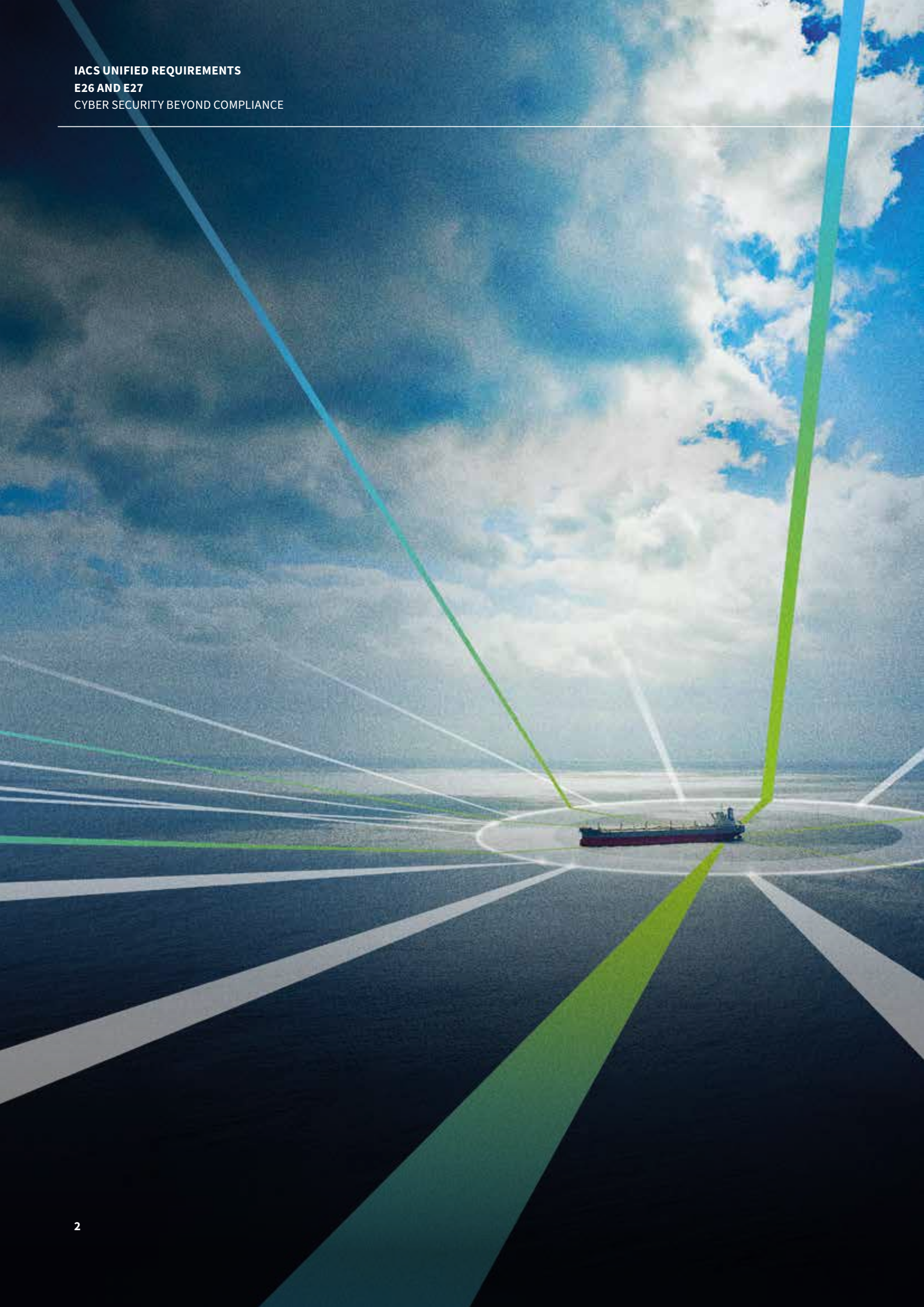


IACS unified requirements E26 and E27 **Cyber security beyond compliance**

ClassNK

Cyber Security | inmarsat



IACS unified requirements **E26 and E27**

Cyber security beyond compliance

Contents

Introduction

As shipping companies worldwide look to reap the rewards of advanced shipboard technologies to support digitalisation, decarbonisation, and crew welfare initiatives, data usage is soaring. According to the latest Inmarsat statistics, data consumption by commercial vessels on Inmarsat's network rose 37% in 2023 vs 2022, and 13% on offshore supply vessels during the same period.

The increasing digitalisation and interconnection of the maritime industry present opportunities to enhance onboard safety, operational efficiency, and environmental sustainability. However, it also leaves vessel networks susceptible to cyber threats – and with cyber incidents growing in frequency, sophistication, and severity, ship owners and ship managers should prioritise integrating security into their connectivity strategy.

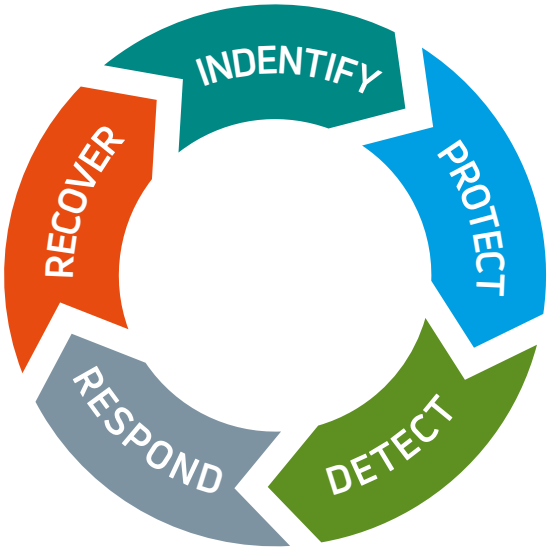
To reduce the occurrence and impact of maritime cyber incidents, the International Association of Classification Societies (IACS) has issued two unified requirements (URs): UR E26 – 'Cyber Resilience of Ships' – and UR E27 – 'Cyber Resilience of Onboard Systems and Equipment'. The URs aim to establish minimum requirements for the cyber resilience capabilities of newbuild vessels and their connected systems, respectively.

Unified Requirement E26

Cyber resilience of vessels

The primary objective of UR E26 is to help maritime organisations to establish and maintain a secure onboard environment. This is divided into five sub-goals corresponding with the five functions of the National Institute of Standards and Technology's Cybersecurity (NIST) Framework, as summarised below:

NIST framework five functions and sub-goals



IDENTIFY	Develop an understanding of cyber security risks to facilitate their identification.
PROTECT	Establish safeguards to protect the ship from cyber attacks.
DETECT	Implement measures for detecting cyber incidents on board.
RESPOND	Set up a protocol for responding to detected cyber attacks.
RECOVER	Adopt procedures to recover any capabilities and/or services impaired by a cyber incident.

Demonstrating compliance

The documentation required for demonstrating compliance with UR E26 relates to three stages of the vessel lifecycle: design and construction, commissioning, and operation. Demonstrating compliance with E26 during the first two phases is the responsibility of the systems integrator – whether the ship builder or an appointed third party – with responsibility passing to the ship owner at the operation phase.

Design and construction

To demonstrate compliance with UR E26 at the design and construction phase, the systems integrator must submit the following three documents to the classification society (The classification society may request the submission of other documentation):

1. **Zones and conduit diagram** including a clear indication of the security zones; a simplified illustration of each computer-based system (CBS) indicating the security zone to which it is allocated as well as its physical location; a reference to the approved version of the CBS topology diagrams provided by the suppliers (see below 'Demonstrating compliance with UR E27', item 2); and illustrations of network communication between systems within a security zone, between systems in different security zones, and between systems in a security zone and untrusted networks.
2. **Vessel asset inventory** covering hardware and software – application programs, any operating systems, firmware, and other software components – of the CBSs relevant to E26; and networks connecting these systems to each other and to other CBSs on board or ashore.

3. **Cyber security design description** providing information, summarising security functions embedded on the CBSs, and added to the networks, as well as the instructions of their security configurations and secure use.

Commissioning
By the time of commissioning, the systems integrator shall submit to the classification society a **ship cyber resilience test procedure** demonstrating that the security zones on board meet criteria set out in the approved documents.

Operation
In the operation phase, the ship owner must submit a **ship cyber security and resilience programme** describing procedures to manage technical and organisational security countermeasures to maintain a secure onboard environment as established at the time of delivery and also to manage any changes during the ship's operational life.

The primary objective of UR E26 is to help maritime organisations to establish and maintain a secure onboard environment based on an effective cyber-risk management system.

Unified Requirement E27

Cyber resilience of onboard systems and equipment

UR E27 aims to support manufacturers and OEMs of onboard operational systems and equipment in evaluating and improving their cyber resilience. It offers comprehensive instructions relating to security philosophy, documentation, system requirements, secure development lifecycle requirements, and plan approval. Based on and incorporating elements of the International Electrotechnical Commission standard IEC 62443, E27's system requirements cover 30 security capabilities required by all CBSs and 11 additional security capabilities required by CBSs that share an interface with untrusted networks.

Demonstrating compliance

Demonstrating compliance with UR E27 requires the submission of the following documents (The classification society may request the submission of other documentation):

1. **CBS asset inventory** including a list of hardware components detailing the manufacturer and model and providing a short description of their functionality; physical interfaces; the name/type of system software and its version and patch level; and supported communication protocols.
2. **CBS topology diagrams** comprising a physical topology diagram illustrating the physical architecture of the system and a logical topology diagram illustrating the data flow between system components.
3. **Description of security capabilities** demonstrating how the CBS meets required security capabilities with its hardware and software components.
4. **Test procedure of security capabilities** describing how to demonstrate, through testing, that the system complies with requirements.
5. **Security configuration guidelines** describing recommended configuration settings of the security capabilities and specifying default values.

UR E27 aims to support maritime organisations in evaluating and improving their cyber resilience.

The class perspective

According to ClassNK, an IACS member, the implementation of URs E26 and E27 will provide full visibility of a newbuild vessel's computer assets and network infrastructure throughout its life. It will also ensure that IACS-classed ships have been delivered with a required minimum level of cyber resilience capabilities regardless of the vessel's type or technical specifications.

However, ClassNK also acknowledges several limitations of the new URs. From the society's perspective, best practice in addressing cyber security requirements is to take a risk-based approach, with cyber-risk controls to be decided and deployed following a thorough risk assessment on the asset onboard, considering risk factors such as the safety criticality and connectivity of the asset, the awareness and capabilities of the crew and shore-personnel, voyage patterns, cargo carried and other factors that may be found necessary by the owner. Yet since the URs are intended to achieve uniform application, applicable systems and corresponding requirements have been predetermined to form only a risk-assessment on the safety criticality. As a result, additional cyber-risk controls may be necessary – particularly for vessels with a high degree of systems integration and interconnectivity. ClassNK also underlines that it is also essential that the onboard operation is governed by established policy and procedures. Human factors should be carefully considered. With humans having the potential to become either the weakest or the strongest link in the chain, fostering cyber hygiene through training, while establishing clear roles and responsibilities, plays a pivotal role in creating a cyber resilient organisation capable of responding to the growing threat of network attacks.

Capturing the cyber security challenges with regard to the growing connected ships, ClassNK will work proactively with the technology enablers and adopters of the technologies to develop and provide services to ensure cyber resilient digital transformation of the industry. ClassNK will also update its existing ClassNK Guidelines on Cyber Security Management to help cyber security champions streamline risk-based cyber security controls effectively by people, process and technology and further integrate them with the organisation's strategy and operations.

The other aspect to be noted in this paper, ClassNK continues, is requirements in the "Detect" and "Respond" elements of the cyber resilience goals included in UR E26 are quite limited and heavily dependent on human operation. As higher-speed and lower-latency connectivity becomes more widespread, digital technologies to support or automate vigilance over the ship's networks and CBSs can be applied and effective.

In the immediate term, vessels using LEO services are also likely to be more attractive targets for malicious attacks. Inmarsat emphasises that this makes it all the more imperative that they are protected and properly secure in their onboard network and IT infrastructure, for example by using solutions like Fleet Secure UTM.

To be better prepared for the future, ClassNK's approach is to collaborate continuously with industry leaders in order to establish the capabilities required of the technology and processes that effectively monitor the security of a vessel's OT network from onshore.

Class surveys

ClassNK

E26

Ship's lifecycle	Design & construction	Commissioning	Operational
Responsibility	Shipbuilder	Shipbuilder	Ship owner
Documents and demonstration	Zones and conduit diagram Vessel asset inventory Cyber security design description	Ship cyber resilience test procedure	Ship cyber security and resilience program

E27

System asset inventory	Description of security capabilities	System maintenance plan
System topology diagrams	System configuration guidelines	System document to support incident response and recovery

Inmarsat key recommendations

Inmarsat believes that while IACS URs E26 and E27 will play an important role in helping maritime organisations to strengthen their cyber defences and develop comprehensive risk-management policies, companies should look beyond compliance with the URs and take a more holistic approach to onboard cyber security. The connectivity solutions provider recommends that organisations focus on, and invest in, three key areas: people and culture, network-connected systems and services, and an incident-response plan.

People and culture

Feedback from Inmarsat security operations centres (SOCs) reveals that phishing attacks are the most frequent type of cyber incident. Companies should therefore pay close attention to their people and organisational culture, investing, for example, in training and awareness programmes and implementing standards such as ISO/IEC 27001. They should also closely assess suppliers' risk-management practices and ensure user privileges are correctly assigned.

IACS REGULATION	NIST FUNCTION	REQUIREMENTS	FS UTM FUNCTION	DESCRIPTION
E26 Cyber Resilience of Ships	Identify & Protect	Ships must have the capability to identify and protect against potential cyber threats	Firewall and Intrusion Prevention Systems (IPS)	Fleet Secure UTM monitors and controls network traffic to prevent unauthorized access and detect malicious activity
			Gateway AV	Regular scanning and real-time protection against viruses and malware ensure the ship's systems are secure
	Detect	Ships must be able to detect cyber incidents in a timely manner	Real-time Network Monitoring / SOC	Continuous monitoring of network activities helps in the early detection of suspicious activities or potential cyber threats
			Intrusion Detection Systems (IDS)	This function alerts operators about unauthorized access attempts or unusual network behaviour
	Response & Recovery	Ships need to have measures in place to respond to and recover from cyber incidents	Automated Alerts /Incident Response (SOC)	Predefined response protocols (such as alerts), automate the mitigation of detected threats, reducing response times and minimizing damage. 24/7 SOC helps with timely incident response
E27 Cyber Resilience of On-board Systems and Equipment	Identify & Protect	On-board systems must use secure communication protocols to protect data integrity and confidentiality	User Authentication (Captive Portal) and Access Control	Role-based access control (RBAC) ensures that only authorized personnel can access network and critical systems
		Implement strong access controls and authentication mechanisms to restrict access to critical systems		
		Conduct regular security assessments and keep systems updated to mitigate vulnerabilities	Advanced Security Reporting	Regular vulnerability scans via reports identify and prioritize security risks/updates

By integrating these features, the Fleet Secure Portfolio can contribute significantly to meeting IMO cyber security regulations, which are designed to enhance the resilience of maritime systems against cyber threats. The portfolio provides a centralized and effective approach to cyber security, helping shipping companies comply with regulatory requirements and protect critical maritime infrastructure.

Network-connected systems and services

Vessels have numerous potential attack surfaces, and maintaining cyber resilience across all of them may not be feasible from a cost and/or time perspective. Inmarsat therefore recommends a risk-management approach that involves identifying onboard assets, assessing risks, deciding which areas require investment, and implementing security measures accordingly.

Incident-response plan

While following cyber security regulations and best practices is critical to reducing the risk of breaches, it is prudent to assume that the threat cannot be controlled through compliance alone. Maritime organisations should therefore have a robust response plan in place to ensure swift recovery from network attacks and to keep financial losses to a minimum.

Companies should look beyond compliance with the URs and take a more holistic approach to onboard cyber security.

Makiko Tani,
Deputy Manager, Cyber Security, ClassNK

Laurie Eve,
Chief of Staff, Inmarsat Maritime

Inmarsat solution

Fleet Secure

Inmarsat's Fleet Secure portfolio helps maritime organisations to comply with cyber security regulations including the new IACS URs while supporting meaningful enhancements across the key three areas described above.

For instance, **Fleet Secure Endpoint** allows users to protect network-connected onboard systems and evaluate risks using the Risk Assessment Report feature. The endpoint-security solution includes access to the Fleet Secure Cyber Awareness training programme, which helps companies to minimise risk by ensuring crew are aware of vulnerabilities and suspicious online behaviour. The crew training completion rate can be tracked by companies, and the course material is updated frequently.

Meanwhile, **Fleet Secure Unified Threat Management (UTM)** comprises a suite of network security tools consolidated on a single device, designed to continuously inspect, detect and protect all the data traffic going to and from a vessel and backed by a dedicated SOC. Intelligently scanning all connected systems for malicious traffic, UTM facilitates the continuous inspection of the entire vessel network as well as the detection and monitoring of threats.

Deployed as part of a holistic, risk-based approach, Inmarsat Fleet Secure enables organisations to integrate cyber security into their connectivity strategy to support regulatory compliance and keep their assets – and people – safe from online threats.

Inmarsat's **Fleet Secure** portfolio helps maritime organisations to comply with cyber security regulations including the new IACS URs while supporting meaningful enhancements across the key three areas described above.

Contact

For further information and questions, please contact the Inmarsat Maritime team: maritime@inmarsat.com

inmarsat.com