IMO cyber guidelines (Rev.4): a terminal's checklist

Reference: **MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 28 May 2026**

One line per point of the guidelines. For each point, read what Rev.4 asks, decide who owns it in your terminal, and write down where the evidence is kept. Mark each line as in place, partial, missing or not applicable, and use the ISPS column to file the point in your port facility security assessment or plan when it belongs there.

Scope. The guidelines are primarily intended for ships (Rev.4, 2.3.1), but they cover ship-port interfaces and the systems that connect ships to shore (2.2.1 .8 and .9, 3.2, 3.5.2), they name the IAPH Cybersecurity Guidelines for Ports and Port Facilities among the references (4.3.4), and they defer to the requirements of each Administration (1.3, 4.1). For the port facility itself, the mandatory frame is the ISPS Code: its port facility security assessment covers « radio and telecommunication systems, including computer systems and networks » (Part B, 15.3.5).

Status

• in place · the evidence exists, is dated and someone owns it

• partial · the practice exists but the evidence is missing, out of date or covers only part of the systems

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal: _____ · date: _____

Point	Rev.4	ISPS Code	Status	Owner
G1 · An accountable person for cybersecurity	3.5.1.1	Part A 17.1 and 16.3.10		
G2 · Authority, support and competence for that person	3.5.1.2	Part A 17.3		
G3 · Senior management leads and is trained	3.3	–		
G4 · Business continuity, disaster recovery and crisis management	3.5.1	Part A 16.3.3		
I1 · Critical systems, their dependencies and supply chains	3.5.2.1	Part A 15.5.1 · Part B 15.3.5		
I2 · Inventory of digital systems and network connections	3.5.2.2	Part B 15.3.5		
I3 · Risk assessment of the critical systems	3.5.2.3	Part A 15.4 and 15.5.2 to 15.5.4		
I4 · Gap assessment against a target posture	3.4	–		
P1 · Unique accounts, separate admin accounts, leavers removed	3.5.3.1	Part A 16.3.2		
P2 · Default passwords, password policy, multi-factor authentication	3.5.3.2	Part B 16.3.2 and 16.8.4		
P3 · Internet exposure and OT/IT segmentation	3.5.3.3 · 2.2.2	Part B 15.3.5		
P4 · Hardware and software approval, secure acquisition, vulnerability handling	3.5.3.3 · 3.8	–		
P5 · Security logs collected and stored securely	3.5.3.3	Part A 16.3.9 · 17.2.8		
P6 · Firewalls and anti-malware at every connection, ship/port interfaces first	3.5.3.4	Part A 16.3.7		
P7 · Removable media controlled	3.5.3.5	–		
P8 · Annual training for all, OT training for OT users, tested by drills	3.5.3.6 · 3.5.4.2 · 3.5.5.3 · 3.5.6.2	Part A 18.1 to 18.4 · Part B 18.5 and 18.6		
P9 · Backups, software updates and an incident response plan	3.5.3.7	Part A 16.3.3		
P10 · Supply chain security policy for critical systems	3.5.3.8 · 2.2.6	–		
P11 · Audits and periodic review of the measures	3.5.3.9	Part A 16.3.8, 16.3.13 and 16.4		
P12 · The cyber documents protected	3.6	Part A 16.3.11, 16.7 and 16.8		
D1 · Know the relevant threats and monitor for them	3.5.4 · 3.5.4.1	Part A 15.4 and 15.5.2		
R1 · Report incidents within the required time frames	3.5.5.1	Part A 16.3.9 · 17.2.8		
R2 · Records of cyber incidents	3.5.5.2	Part A 17.2.8		
R3 · Contain the incident and practise the response	3.5.5	Part A 16.3.3 · Part B 18.6		
C1 · Recovery strategies for the critical systems	3.5.6 · 3.5.6.1	Part A 16.3.3		
C2 · Root cause analysis after each incident	3.5.6.3	Part A 17.2.5		

Govern (Rev.4, 3.5.1)

Strategy, roles and business continuity, including backups, disaster recovery and crisis management.

G1 · An accountable person for cybersecurity (Rev.4 3.5.1.1)

What Rev.4 asks: Designate a person or entity accountable for the planning, resourcing and execution of cybersecurity activities.

For a terminal: Name one owner for cyber risk across IT and operational systems (gate, yard, cranes, access control, cameras), not only for office IT. If this is not the port facility security officer, write down how the two work together.

Evidence to hold: [ ] A dated designation letter or organisation chart naming the person or entity · [ ] The scope of that role, covering IT and operational technology (OT) · [ ] How the cyber owner and the port facility security officer (PFSO) coordinate

ISPS Code Part A 17.1 and 16.3.10: The PFSO is designated and identified in the plan with 24-hour contact details; the plan can name the cyber contact the PFSO calls.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G2 · Authority, support and competence for that person (Rev.4 3.5.1.2)

What Rev.4 asks: Give the designated person or entity the necessary authority and support, and make sure they have sufficient knowledge and expertise in cyber risk management.

For a terminal: The cyber owner can stop a risky change, get a budget decision and reach management. Their competence is shown, not assumed.

Evidence to hold: [ ] The written mandate or delegation of authority · [ ] The budget or resource decisions for cybersecurity (meeting minutes) · [ ] Training certificates or a short competence record for the person

ISPS Code Part A 17.3: The ISPS Code uses the same idea for the PFSO: « given the necessary support to fulfil the duties ».

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G3 · Senior management leads and is trained (Rev.4 3.3)

What Rev.4 asks: Cyber risk management starts at senior management level: management follows relevant training, embeds a culture of cyber risk awareness at all levels, and keeps the regime in continuous operation with feedback mechanisms.

For a terminal: The management of the terminal is briefed on cyber risk, has taken a short training, and reviews the cyber position at a set interval.

Evidence to hold: [ ] Management training attendance (date, names or roles) · [ ] Minutes of management meetings where cyber risk was reviewed · [ ] The feedback loop: how incidents, audits and drills reach management

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G4 · Business continuity, disaster recovery and crisis management (Rev.4 3.5.1)

What Rev.4 asks: Govern includes ensuring business continuity, such as backup management and disaster recovery, and crisis management.

For a terminal: A continuity plan that says how the terminal keeps working (gate, vessel and yard operations) when a critical system is lost, who decides, and how the crisis team is called.

Evidence to hold: [ ] The business continuity plan covering the critical systems, with its date and owner · [ ] The disaster recovery plan for those systems · [ ] The crisis team list and call-out procedure

ISPS Code Part A 16.3.3: The plan must cover procedures for responding to security threats or breaches, « including provisions for maintaining critical operations of the port facility or ship/port interface ».

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Identify (Rev.4, 3.5.2)

The systems, their dependencies and supply chains, the inventory and the risk assessment.

I1 · Critical systems, their dependencies and supply chains *(Rev.4 3.5.2.1)*

What Rev.4 asks: Identify the systems, assets, services, data and capabilities, and the interdependencies between safety-critical systems (including the information flow), whose disruption poses risks, including those related to the software and hardware supply chains.

For a terminal: List the systems the terminal cannot run without, how data flows between them, and which suppliers they depend on: for example the terminal operating system, gate and appointment systems, crane and equipment controls, access control and video, and the links to shipping lines, customs and the port community system.

Evidence to hold: [ ] The list of critical systems with an owner for each · [ ] A data-flow or dependency diagram between them · [ ] The suppliers and service providers each critical system depends on

ISPS Code Part A 15.5.1 · Part B 15.3.5: The port facility security assessment identifies and evaluates the important assets and infrastructure to protect, and addresses « radio and telecommunication systems, including computer systems and networks ».

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I2 · Inventory of digital systems and network connections *(Rev.4 3.5.2.2)*

What Rev.4 asks: Establish and maintain an inventory of digital systems, and identify internal and external system dependencies and network connections.

For a terminal: Rev.4 writes « on board the ship »; the terminal equivalent is an inventory of its IT and OT systems and of every connection to the outside: vessels, shipping lines, customs, rail and road partners, and suppliers' remote access.

Evidence to hold: [ ] The asset inventory (IT and OT), with the date of the last update · [ ] A network diagram showing the zones and the connections between them · [ ] The list of external connections, with the purpose and owner of each

ISPS Code Part B 15.3.5: The inventory is the input the assessment needs for computer systems and networks.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I3 · Risk assessment of the critical systems *(Rev.4 3.5.2.3)*

What Rev.4 asks: Carry out a risk assessment of the systems, services, assets, data and capabilities critical to operations whose sudden failure may result in hazardous situations: identify cyber threats and vulnerabilities, and assess the likelihood and impact of a cyber incident on safety, availability, integrity and confidentiality.

For a terminal: A dated cyber risk assessment of the critical systems, with the threats, the weaknesses found and the treatment decided for each risk.

Evidence to hold: [ ] The risk assessment report, with its date and method · [ ] The risk register with likelihood, impact, owner and treatment · [ ] The date of the next review

ISPS Code Part A 15.4 and 15.5.2 to 15.5.4: The port facility security assessment identifies threats and their likelihood, countermeasures and weaknesses, « including human factors », and is reviewed when threats or the facility change.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I4 · Gap assessment against a target posture *(Rev.4 3.4)*

What Rev.4 asks: Assess and compare the organisation's current and desired cyber risk management postures, to reveal gaps and address them through a risk-based approach.

For a terminal: Pick a reference (the guidelines name ISO/IEC 27001, the NIST framework 2.0 and the IAPH guidelines for ports, among others), measure where the terminal stands against it, and turn the gaps into a dated action plan.

Evidence to hold: [ ] The gap assessment against the chosen reference, dated · [ ] The action plan with owners and target dates

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Protect (Rev.4, 3.5.3)

The minimum controls: accounts, passwords and MFA, exposure, logs, segmentation, media, training, backups, supply chain, audits.

P1 · Unique accounts, separate admin accounts, leavers removed (Rev.4 3.5.3.1)

What Rev.4 asks: Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deactivate accounts for departing employees or users.

For a terminal: No shared logins on the terminal systems (including the crane, gate and access-control consoles where technically possible), separate administrator accounts, and a leaver procedure that also covers contractors and suppliers.

Evidence to hold: [ ] The account review of the critical systems, with the date and the shared accounts left (and why) · [ ] The list of privileged accounts and who holds them · [ ] The leaver procedure and the record of the last leavers processed (badges, tokens, accounts)

ISPS Code Part A 16.3.2: The plan covers measures to prevent unauthorised access to the facility and its restricted areas; the badge and access-control system that enforces them is itself a computer system with accounts.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P2 · Default passwords, password policy, multi-factor authentication (Rev.4 3.5.3.2)

What Rev.4 asks: Change all default passwords on all devices, enforce a strong password policy, protect against brute force and phishing, and use multi-factor authentication or continuous authentication, secured communications and secured emergency communication systems, where appropriate.

For a terminal: Default passwords changed on cameras, controllers, switches and appliances; multi-factor authentication on remote access, administrator accounts and e-mail first.

Evidence to hold: [ ] The record that default passwords were changed, per device type · [ ] The password policy · [ ] The list of systems with multi-factor authentication, and those without (and why) · [ ] The secured means used for security and emergency communications

ISPS Code Part B 16.3.2 and 16.8.4: The plan details the communication systems that keep the security organisation working and in contact with ships and authorities.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P3 · Internet exposure and OT/IT segmentation (Rev.4 3.5.3.3 · 2.2.2)

What Rev.4 asks: Limit exploitable services on the Internet and segment OT device networks from IT networks; OT systems should be segmented from IT systems and protected from Internet-facing systems.

For a terminal: Know what the terminal exposes to the Internet, close what is not needed, and keep crane, equipment and other operational networks apart from the office network.

Evidence to hold: [ ] The result of the last external exposure check, with its date · [ ] The firewall rule review between the zones · [ ] The network diagram showing the OT zones separated from IT

ISPS Code Part B 15.3.5: Exposure and segmentation are part of the computer systems and networks the assessment addresses.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P4 · Hardware and software approval, secure acquisition, vulnerability handling (Rev.4 3.5.3.3 · 3.8)

What Rev.4 asks: Establish a hardware and software approval process, and ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure. Equipment and systems should be designed and tested to international standards for cyber resilience.

For a terminal: Nothing joins the network without approval; security requirements are written into tenders and contracts; the terminal follows the security advisories of its suppliers and applies the fixes.

Evidence to hold: [ ] The approval procedure and its log for new hardware and software · [ ] The security clauses used in purchases (see the RFP cyber checklist) · [ ] The tracking of supplier security advisories for the systems in use

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P5 · Security logs collected and stored securely (Rev.4 3.5.3.3)

What Rev.4 asks: Collect and securely store logs for intrusion detection and incident response.

For a terminal: Logs from the critical systems, the firewalls and the remote-access paths are collected in one place, kept long enough for an investigation, and protected from change.

Evidence to hold: [ ] The list of log sources collected · [ ] The retention period decided by the terminal, and where the logs are stored · [ ] Who can read, and who cannot alter, the logs

ISPS Code Part A 16.3.9 · 17.2.8: Logs support the reporting of security incidents and the records the PFSO keeps.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P6 · Firewalls and anti-malware at every connection, ship/port interfaces first (Rev.4 3.5.3.4)

What Rev.4 asks: Implement security measures (such as firewall or antivirus) for digital systems and devices that have access to the Internet or the intranet, or interact with third-party or landside systems, particularly those of ship/port interfaces; implement policies and procedures on the use of cryptography.

For a terminal: Every link with a vessel, a shipping line or a partner goes through a controlled point; endpoints are protected; encryption is used for data in transit on those links.

Evidence to hold: [ ] The list of ship/port and partner interfaces with the control applied to each · [ ] The anti-malware coverage of the endpoints and servers · [ ] The cryptography policy

ISPS Code Part A 16.3.7: The plan holds the procedures for interfacing with ship security activities.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P7 · Removable media controlled (Rev.4 3.5.3.5)

What Rev.4 asks: Establish controls to protect systems from the use of unauthorised removable media.

For a terminal: USB keys and laptops brought by staff, crews and maintenance suppliers are controlled before they touch operational systems.

Evidence to hold: [ ] The removable media policy · [ ] The technical control in place (blocking, scanning station) and where

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P8 · Annual training for all, OT training for OT users, tested by drills (Rev.4 3.5.3.6 · 3.5.4.2 · 3.5.5.3 · 3.5.6.2)

What Rev.4 asks: Mandate annual basic cybersecurity training for all employees and OT-specific training for OT users, covering cyber hygiene and how to recognise, respond to and recover from a cyber incident; test the knowledge occasionally, for example through drills and exercises.

For a terminal: A yearly training plan for everyone, a specific one for operators and engineers of the operational systems, and a cyber scenario in the drills the terminal already runs.

Evidence to hold: [ ] The training plan and attendance records, per year · [ ] The OT-specific training records · [ ] The report of the last drill or exercise with a cyber scenario

ISPS Code Part A 18.1 to 18.4 · Part B 18.5 and 18.6: The ISPS Code already requires training, drills and exercises for the port facility (Part B guidance: drills at least every three months, exercises at least once each calendar year with no more than 18 months between them); a cyber scenario can be one of them.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P9 · Backups, software updates and an incident response plan (Rev.4 3.5.3.7)

What Rev.4 asks: Perform regular system backups and software updates, and develop and maintain incident response plans.

For a terminal: Backups of the critical systems, including a copy that an attacker on the network cannot reach, restore tests, updates applied on a schedule, and a written incident response plan.

Evidence to hold: [ ] The backup schedule and the report of the last restore test · [ ] The update status of the critical systems · [ ] The incident response plan, with its date and owner

ISPS Code Part A 16.3.3: Responding to security threats while maintaining critical operations is a required part of the plan.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P10 · Supply chain security policy for critical systems (Rev.4 3.5.3.8 · 2.2.6)

What Rev.4 asks: Establish policies on software and hardware supply chain security for the systems and assets identified as critical, and consider the risks posed by third-party vendors, embedded systems and maintenance devices.

For a terminal: A written policy for the suppliers of the critical systems: what they must prove before connecting, how their remote access is controlled, and what the contract says about patches, incidents and exit.

Evidence to hold: [ ] The supplier security policy · [ ] The list of critical suppliers and how each reaches the network · [ ] The security clauses of their contracts (see the vendor onboarding grid)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P11 · Audits and periodic review of the measures (Rev.4 3.5.3.9)

What Rev.4 asks: Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.

For a terminal: An audit or test of the cyber measures at a set interval, and a review that updates the measures and this checklist.

Evidence to hold: [ ] The audit plan and the last audit or test report · [ ] The record of the last review and the changes it made

ISPS Code Part A 16.3.8, 16.3.13 and 16.4: The plan provides for its periodic review and its auditing; internal auditors are independent of the activities audited unless that is impracticable.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P12 · The cyber documents protected (Rev.4 3.6)

What Rev.4 asks: Protect any documents developed for these functional elements by procedures aimed at preventing unauthorised access, deletion, destruction or amendment.

For a terminal: Network diagrams, inventories, risk assessments and this checklist are sensitive: keep them in one controlled place with access rights and version history.

Evidence to hold: [ ] Where the documents are stored, and who has access · [ ] The version history or change log

ISPS Code Part A 16.3.11, 16.7 and 16.8: Almost the same words as the ISPS Code for the plan itself: protected from unauthorised access or disclosure, and, in electronic format, from « unauthorised deletion, destruction or amendment ».

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Detect (Rev.4, 3.5.4)

Know the relevant threats and watch the systems for them.

D1 · Know the relevant threats and monitor for them (Rev.4 3.5.4 · 3.5.4.1)

What Rev.4 asks: Maintain a list of relevant threats and of threat actor tactics, techniques and procedures, and actively monitor systems for those threats; implement measures to detect unintended activity and identify a cyber incident in a timely manner.

For a terminal: A short list of the threats that matter to the terminal, and monitoring that would see them on the critical systems, with a named person who looks at the alerts.

Evidence to hold: [ ] The threat list, with the date of its last update · [ ] The monitoring coverage: which systems, which alerts, who reviews them and when

ISPS Code Part A 15.4 and 15.5.2: The assessment identifies possible threats and is reviewed as threats change.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Respond (Rev.4, 3.5.5)

Report within the required time frames, keep records, contain the incident.

R1 · Report incidents within the required time frames (Rev.4 3.5.5.1)

What Rev.4 asks: Report incidents to the necessary parties within the required time frames as defined by the Administration.

For a terminal: Know who must be told and how fast: the national authority, the computer security incident response team, and, in the EU where NIS2 applies, the early warning within 24 hours and the notification within 72 hours.

Evidence to hold: [ ] The reporting procedure with recipients and time frames · [ ] The up-to-date contact list

ISPS Code Part A 16.3.9 · 17.2.8: The plan holds the procedures for reporting security incidents; the PFSO reports to the relevant authorities and keeps records of occurrences.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R2 · Records of cyber incidents (Rev.4 3.5.5.2)

What Rev.4 asks: Keep records of cyber incidents.

For a terminal: An incident register, including the incidents that were contained quickly.

Evidence to hold: [ ] The incident register (date, systems, impact, actions, closure)

ISPS Code Part A 17.2.8: The PFSO maintains records of occurrences which threaten the security of the port facility.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R3 · Contain the incident and practise the response (Rev.4 3.5.5)

What Rev.4 asks: Develop, implement and practise activities and plans to restore systems needed for shipping and ship-port operations, and minimise the effect of a detected incident on other parts of the systems.

For a terminal: Playbooks that say how to isolate a zone or a supplier link without stopping the whole terminal, tested in an exercise.

Evidence to hold: [ ] The response playbooks for the main scenarios · [ ] The report of the last exercise and the actions it produced

ISPS Code Part A 16.3.3 · Part B 18.6: Exercises under the ISPS Code test communication, coordination, resource availability and response.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Recover (Rev.4, 3.5.6)

Restore the critical systems and fix the root cause.

C1 · Recovery strategies for the critical systems (Rev.4 3.5.6 · 3.5.6.1)

What Rev.4 asks: Develop, maintain and implement strategies for the recovery and reinstatement of essential business or mission critical assets or systems that might be impacted by a cyber incident.

For a terminal: The order in which systems come back, the recovery times the terminal sets for itself, and the manual fallback for gate and vessel operations while systems are down.

Evidence to hold: [ ] The recovery plan with the restoration order and the target times set by the terminal · [ ] The manual fallback procedures, and when they were last used or tested

ISPS Code Part A 16.3.3: Maintaining critical operations of the port facility and the ship/port interface.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C2 · Root cause analysis after each incident (Rev.4 3.5.6.3)

What Rev.4 asks: Carry out root cause analysis of cyber incidents, to resolve the underlying issues and vulnerabilities and prevent recurrence.

For a terminal: After each significant incident, a short analysis of why it happened, and actions tracked until closed.

Evidence to hold: [ ] The root cause analysis reports · [ ] The action tracker and its closure dates

ISPS Code Part A 17.2.5: The PFSO recommends modifications to the plan to correct deficiencies.

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

IMO, MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 2026-05-28.
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

IMO, Maritime cyber risk (web page), read 2026-11-11.
https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

ISPS Code, Parts A and B, as reproduced in Annexes II and III of Regulation (EC) No 725/2004 on enhancing ship and port facility security, 2004-03-31. https://eur-lex.europa.eu/eli/reg/2004/725/oj

IMO, SOLAS XI-2 and the ISPS Code (web page), read 2026-11-11.
https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Directive (EU) 2022/2555 (NIS2), Article 23: reporting obligations, 2022-12-14.
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/compliance-center/imo-cyber-guidelines-checklist/ . Generic: no terminal, port, client or vendor is named and no figure is invented. This checklist is not legal advice and does not replace the text of the guidelines, the ISPS Code or your Administration's requirements; Port Cyber Alliance does not certify or audit terminals.