Port Cyber Alliance · free tool

The cyber checklist for your port software RFP

Copy the eight requirements into the security annex of your request for proposal, set the values in brackets, and ask every bidder to answer each one with evidence. Score each answer from 0 to 3 with the guide below, multiply by the weight, and exclude any bid that scores 0 on a must-have requirement.

Score scale

- 0 · no answer, a refusal, or an answer that contradicts the requirement
- 1 · a commitment in words, without evidence
- 2 · a commitment with evidence (a document, a report summary, a screenshot, a reference procedure)
- 3 · evidence, and the bidder accepts the requirement as a contract clause with a remedy

Formula: weighted score = sum(weight × score) ÷ (3 × sum(weight)) × 100 · any must-have at 0 excludes the bid

Summary sheet (one per bidder) · bidder: _____

Requirement	Must-have	Weight	Score 0-3	Weighted
1. Security patches	yes	[3]		
2. Penetration tests	no	[2]		
3. Hosting and data location	no	[2]		
4. Reversibility and exit	yes	[3]		
5. Security logs	no	[2]		
6. Multi-factor authentication	yes	[3]		
7. Incident notification	yes	[3]		
8. Subcontractors	no	[2]		
Total				

Weights in brackets are defaults: set your own before you publish the RFP.

1. Security patches · must-have

Unpatched software is one of the ways into a terminal. The IMO guidelines name system patching among the sources of vulnerability, and NIS2 asks for security in the acquisition and maintenance of systems, including vulnerability handling and disclosure.

Clause to write in the RFP

> The supplier fixes security vulnerabilities in its software within [x] days for critical, [y] days for high and [z] days for other severities, counted from public disclosure or from the supplier's own discovery. It publishes a vulnerability disclosure policy, tells the buyer of every security fix that concerns the delivered version, and provides a software bill of materials (SBOM) in a standard machine-readable format on request.

Evidence to request: The patch policy with the time per severity · The vulnerability disclosure policy (public URL) · The last security advisories published for the product · An SBOM sample for the proposed version

Score	When
0	No commitment on time, or « patches are delivered with the next release »
1	Times stated but no policy or advisory to show
2	Written policy, published disclosure policy and real advisories
3	As 2, the times accepted in the contract with a remedy, SBOM delivered

Red flags: Security fixes only through a paid upgrade · No way to know whether a published vulnerability concerns your version

Sources: Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08) · CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13)

2. Penetration tests

A penetration test is the closest thing to evidence that the controls work. The buyer cannot audit the code; an independent tester can test the product and the service.

Clause to write in the RFP

> The supplier has the product and its hosting tested by an independent tester at least every [period] and after every major change, shares an executive summary and the remediation status with the buyer, and allows the buyer to have its own test performed on its instance with [notice] notice.

Evidence to request: The executive summary of the last test (date, scope, tester's independence) · The remediation status of the findings · The rules for a test ordered by the buyer

Score	When
0	No test, or the supplier refuses to share anything
1	« We test regularly », nothing to show
2	A recent summary with scope and remediation status
3	As 2, plus the buyer's own test allowed in the contract

Red flags: A test older than the version on offer · A scope that leaves out the hosting or the interfaces you will use

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers (written for healthcare; its procurement life-cycle method applies to any buyer) (2026-07-22) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13)

3. Hosting and data location

The terminal stays responsible for its data, and often for personal data of drivers and staff. It must know where the data sits, who hosts it, and who can read it.

Clause to write in the RFP

> The supplier states where the buyer's data and its backups are hosted (countries and hosting providers), encrypts them in transit and at rest, keeps the buyer's data separate from other customers', and gives [notice] notice before any change of country or hosting provider.

Evidence to request: The hosting diagram with countries and providers · Encryption in transit and at rest, and who holds the keys · The backup plan and the last restore test · Security certifications of the hosting, if any, with their scope

Score	When
0	Location unknown or not disclosed
1	Location stated, nothing else
2	Diagram, encryption and backup plan documented
3	As 2, the location and the notice of change in the contract

Red flags: « The cloud » as the only answer on location · Backups never restored in a test

Sources: Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication (2022-12-14) · ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers (written for healthcare; its procurement life-cycle method applies to any buyer) (2026-07-22) · CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13)

4. Reversibility and exit · must-have

A terminal cannot stop when a contract ends. Reversibility is what lets it change supplier, or take the service back, without losing data or operations.

Clause to write in the RFP

> At the end of the contract, for any reason, the supplier hands over all the buyer's data and configuration in a documented open format within [x] days, assists the transition for [period], keeps the service running during it, then deletes the data and confirms the deletion in writing.

Evidence to request: The export format, with its documentation · The exit plan (steps, duration, who does what) · A sample export

Score	When
0	No export, or a proprietary format only
1	Export promised, format not documented
2	Documented open format, written exit plan, sample shown
3	As 2, the exit plan and deletion certificate in the contract

Red flags: An export priced or scoped only at the end of the contract · Data that can only be read by the supplier's own software

Sources: ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers (written for healthcare; its procurement life-cycle method applies to any buyer) (2026-07-22) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication (2022-12-14)

5. Security logs

Without logs, an incident cannot be detected or explained. The IMO guidelines ask to collect and securely store logs for intrusion detection and incident response; CISA asks that security logs come in the baseline product.

Clause to write in the RFP

> The product records security events (sign-ins, failed sign-ins, changes of rights and settings, data exports, administrator and supplier actions), keeps them for at least [period], protects them from change, and lets the buyer export them to its own monitoring tool in a standard format, at no extra cost.

Evidence to request: The list of events logged · The retention period and how logs are protected · The export method (format, protocol) and a sample

Score	When
0	No security log, or logs only on request after an incident
1	Logs exist, no export
2	Documented events, retention and export, sample shown
3	As 2, included in the base price and written in the contract

Red flags: Logging sold as an extra module · Supplier actions on the buyer's instance not logged

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08) · CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13)

6. Multi-factor authentication · must-have

Stolen passwords open more doors than any other method. NIS2 lists multi-factor authentication among the minimum measures, the IMO guidelines ask for it, and CISA asks for it by default and at no extra cost.

Clause to write in the RFP

> Multi-factor authentication is available for every user and enforced for administrators and for the supplier's own staff, with no shared or default accounts. Single sign-on with the buyer's identity provider is supported at no extra cost.

Evidence to request: The authentication methods supported · How the supplier's support staff sign in to the buyer's instance · Single sign-on documentation

Score	When
0	No multi-factor authentication
1	Available but optional for administrators or supplier staff
2	Enforced for administrators and supplier staff, single sign-on available
3	As 2, at no extra cost and written in the contract

Red flags: Single sign-on only in a premium tier · A shared support account

Sources: Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08)

7. Incident notification · must-have

A terminal in scope of NIS2 must send an early warning within 24 hours and a notification within 72 hours of becoming aware of a significant incident. It cannot meet those deadlines if its supplier tells it late.

Clause to write in the RFP

> The supplier notifies the buyer of any security incident that affects or may affect the buyer's service or data within [x] hours of becoming aware of it, through a named contact available 24/7, then sends updates and a final report, and cooperates with the buyer's own notifications to the authorities.

Evidence to request: The incident response procedure (summary) · The 24/7 contact and escalation path · A redacted example of an incident report

Score	When
0	No commitment, or « as soon as possible »
1	A time stated, no procedure or contact
2	Procedure, 24/7 contact and time consistent with your own deadlines
3	As 2, in the contract, with cooperation for authority reports

Red flags: Notification only after the supplier's own investigation is over · Only « confirmed » incidents notified

Sources: Directive (EU) 2022/2555 (NIS2), Article 23: reporting obligations (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13)

8. Subcontractors

The supply chain does not stop at the supplier. NIS2 asks for supply-chain security, including the relationships between each entity and its direct suppliers; the IMO guidelines name third-party vendors and software supply chains.

Clause to write in the RFP

> The supplier lists the subcontractors that host, process or can reach the buyer's data or systems, passes the same security obligations on to them, and gives [notice] notice before adding or changing one, with a right for the buyer to object.

Evidence to request: The list of subcontractors and what each one does · How the obligations are passed on (contract clause) · How the supplier checks them

Score	When
0	No list
1	A list, no obligations passed on
2	List, obligations passed on, checks described
3	As 2, notice and right to object in the contract

Red flags: Offshore support teams not in the list · « Our partners » without names

Sources: Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13)

Sources (public, dated)

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

Directive (EU) 2022/2555 (NIS2), Article 21: supply chain, acquisition and maintenance, multi-factor authentication, 2022-12-14. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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

CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem, 2024-08. https://www.cisa.gov/resources-tools/resources/secure-demand-guide

CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products, 2025-01-13. https://www.cisa.gov/resources-tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting

ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers (written for healthcare; its procurement life-cycle method applies to any buyer), 2026-07-22. https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers

ENISA, Good Practices for Supply Chain Cybersecurity, 2023-06-13. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

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 grid, including commercially and inside your own tender documents, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/rfp-cyber-checklist/ . Generic and anonymised: no terminal, port, client or vendor is named, no figure comes from a real tender. This grid is not legal advice; Port Cyber Alliance does not certify vendors or audit terminals.