Vendor cyber questionnaire

A terminal or a port sends this questionnaire to a software vendor before connecting its software. The vendor answers every question with the scale below, writes what it really does, and attaches the evidence. An honest « planned, with a date and an owner » is better than a vague yes. The terminal reads the answers family by family and asks for the missing evidence.

Answer scale: Yes, with evidence attached · Yes, no evidence yet · Not yet, planned with a date and an owner · No · Not applicable, with the reason

Online form (runs in your browser, sends nothing): https://portcyberalliance.org/vendor-questionnaire/form/

Who asks (the terminal or port)

Terminal or port	
Contact person	
Contact e-mail	
Date sent	
Answers expected by	
Software and connection in scope	

Who answers (the vendor)

Vendor company	
Product and version	
Contact person	
Contact e-mail	
Date answered	

1. Access

Remote access by suppliers is one of the ways into a terminal's network. The terminal wants to know who at your company can reach its systems, how, and how that access ends.

Id	Question	Answer	Answer and evidence
ACC-01	Who in your company can reach our systems or our data, by role, and how many people is that?		
ACC-02	How do they connect (our VPN, a jump host, your own remote tool), and can we approve or cut each session?		
ACC-03	Is multi-factor authentication required for every person, including administrators and support staff?		
ACC-04	Are accounts named and personal, with no shared or default passwords?		
ACC-05	How fast is access removed when someone leaves your team, and how often do you review the list with us?		

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

2. Data

The terminal stays responsible for its data, and often for personal data of drivers, crews and staff. It needs to know what you hold, where, and who can read it.

Id	Question	Answer	Answer and evidence
DAT-01	What data of ours do you store or process, and which of it is personal data?		
DAT-02	In which countries is it hosted, and by which hosting provider?		
DAT-03	Is it encrypted in transit and at rest, and who holds the keys?		
DAT-04	How is our data kept apart from your other customers' data?		
DAT-05	How long do you keep each kind of data, and can we change that?		

Sources: ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01)) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

3. Logs

Without logs, a terminal cannot see what happened in your software, nor send it to its own monitoring. Logging that costs extra or cannot leave your platform is a common blocker.

Id	Question	Answer	Answer and evidence
LOG-01	What do you log (logins, administrator actions, changes of settings, API calls, data exports)?		
LOG-02	How long do you keep the logs, and are they protected against change?		
LOG-03	Can we receive the logs in our own monitoring tool (SIEM), in a standard format, at no extra cost?		
LOG-04	Are the clocks of your systems synchronised, so that times match ours?		

Sources: 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) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

4. Backups

A terminal works around the clock. If your service stops or its data is encrypted by ransomware, the terminal wants to know how fast it comes back and with how much data lost.

Id	Question	Answer	Answer and evidence
BAK-01	How often is our data backed up, and where are the backups kept?		
BAK-02	Are backups separated from the production systems, so that one attack cannot reach both?		
BAK-03	When did you last restore from a backup as a test, and what was the result?		
BAK-04	How long does it take to restore the service, and how much data can be lost at most?		

Sources: 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)

5. Incidents

In the European Union, an operator in scope of NIS2 sends an early warning within 24 hours of becoming aware of a significant incident, and a notification within 72 hours. It can only meet that if its suppliers tell it fast.

Id	Question	Answer	Answer and evidence
INC-01	How and how fast will you tell us about an incident that affects our data or our service?		
INC-02	Who is our contact during an incident, and can we reach them at any hour?		
INC-03	What will your first notice contain, and how will you keep us updated?		
INC-04	Will you help us with our own notifications to the authorities, and share what you learned afterwards?		

Sources: Directive (EU) 2022/2555 (NIS2), Articles 21 and 23 (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

6. Subcontractors

Your suppliers become the terminal's suppliers. The risk does not stop at your company, and the terminal needs to know who else touches its data or its systems.

Id	Question	Answer	Answer and evidence
SUB-01	Which subcontractors (hosting, support, development, monitoring) touch our data or our systems?		
SUB-02	Where are they, and what do they have access to?		
SUB-03	Do your security requirements apply to them in their contracts?		
SUB-04	Will you tell us before you add or change a subcontractor?		

Sources: NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01)) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · Directive (EU) 2022/2555 (NIS2), Articles 21 and 23 (2022-12-14)

7. Penetration tests

A terminal wants proof that someone outside your team has tried to break your software, and that what they found was fixed. It also wants to know how you handle vulnerabilities found later.

Id	Question	Answer	Answer and evidence
PEN-01	When was your software last tested by an independent penetration tester, and what was in scope?		
PEN-02	Can we see a summary of the findings and how each one was fixed?		
PEN-03	May we, or a tester we choose, test the service we use?		
PEN-04	Do you publish a vulnerability disclosure policy, and how fast do you fix critical vulnerabilities?		

Sources: 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) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

8. End of contract

The day the contract ends, the terminal must get its data back, and be sure your company no longer holds it or can reach its systems.

Id	Question	Answer	Answer and evidence
END-01	In which format do we get our data back, and how long do you take?		
END-02	How do you delete our data, including backups, and do you confirm it in writing?		
END-03	How are your accesses, accounts and keys to our systems removed?		
END-04	What help do you give to move to another system?		

Sources: ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

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

NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2022-05 (updated 2024-11-01). https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

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

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

Directive (EU) 2022/2555 (NIS2), Articles 21 and 23, 2022-12-14. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Licence

Questionnaire: Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . Copy, adapt and share it, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/open-source-packages/vendor-questionnaire-open-source/ . What to prepare and model answers for every family: https://portcyberalliance.org/resources/vendor-cyber-onboarding/ . Generic and anonymised: no terminal, port, client or vendor is named. Port Cyber Alliance does not certify vendors or audit terminals.