Port Cyber Alliance · free tool

Cyber maturity grid for a port or a terminal

Five levels, six functions: identify, protect, detect, respond, recover, govern. The functions are the functional elements of the IMO guidelines on maritime cyber risk management (Rev.4, 28 May 2026) and the Functions of the NIST Cybersecurity Framework 2.0 (26 February 2024). The five levels are Port Cyber Alliance's own scale, not a certification.

How to use it. For each of the six functions, read the five levels from the bottom up. Your level is the highest one for which you can show all the evidence, not the one you intend to reach. If you hesitate between two levels, take the lower one. Keep one level per function: the result is a profile, not an average. Then choose a target one level higher on the one or two functions that matter most for your operations, and use the « next step » of your current level as the first item of the plan.

The five levels

Level 1 · Ad hoc: Cyber depends on a few people and on luck. Nothing is written, nobody is accountable.

Level 2 · Started: Some measures exist, mostly on office IT. They are partial, not written down or not kept up to date.

Level 3 · Defined: The measures are written, owned and cover the whole site, operational technology included.

Level 4 · Managed: The measures are tested and measured, and management reviews the results on a schedule.

Level 5 · Adaptive: Tests, exercises and incidents change the measures, and the terminal works with its partners in the port chain.

What moves you to the next level

1 → **2**: Name an owner, and write down what exists. Most of the step is making the invisible visible.

2 → **3**: Write it, extend it to operational technology, and get management to approve it. A measure that only covers office IT stays at level 2.

3 → **4**: Test and measure. A plan that was never exercised, a backup never restored or a control never audited is level 3 at best.

4 → **5**: Learn and share: every exercise and incident changes something, and the port chain partners are part of the work.

Scoring sheet · site: _____ · date: _____

Function	Our level (1-5)	Target level	First step / owner / date
Identify			
Protect			
Detect			
Respond			
Recover			
Govern			

Score on evidence: your level is the highest one for which you can show all the evidence. If in doubt, take the lower level.

Identify

IMO Rev.4: Determine the current cyber risk to ships and ship/port interfaces: systems, assets, data, dependencies, supply chains, risk assessment.

NIST CSF 2.0: The organization's current cybersecurity risks are understood (ID).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	Nobody can list every system the terminal runs on. Knowledge of the TOS servers, gate lanes, crane controllers and vendor connections sits in a few people's heads.	• Nothing beyond invoices and vendor contracts	Write a first list of the systems that would stop the gate, the yard or the quay if they failed, with an owner for each.
2 Started	A list exists for office IT or for the TOS, but operational equipment (cranes, gates, OCR, reefer monitoring) and vendor remote access are missing or out of date.	• A spreadsheet of IT assets • A network diagram more than a year old	Extend the inventory to operational technology and to every external connection, and rank the systems by what they stop when they fail.
3 Defined	One inventory covers IT and operational technology, with an owner, the network connections and the supplier of each system. The systems critical to operations are ranked and a risk assessment was written for them.	• Inventory with OT and vendor connections, and the date of its last update • Written risk assessment of the critical systems • List of the vendors that can reach the site remotely	Update the inventory through change management, and repeat the risk assessment on a schedule and after each major change.
4 Managed	The inventory is updated with every change and compared with what is really seen on the network. The risk assessment is repeated on a schedule and after major changes, and it covers the software and hardware supply chains.	• Change records that update the inventory • A network discovery report compared with the inventory • Dated risk assessments, supplier risk reviews	Feed the risk register with the threat information shared by your port community and the authorities, and map your dependencies on chain partners.
5 Adaptive	The risks include the ship/port interfaces and the dependencies on partners in the port chain (port community system, port authority, shipping lines, hauliers). Shared threat information updates the risk register.	• Risk register entries linked to shared alerts • Dependency map with the chain partners • Minutes of the yearly review	Keep it there: review the profile once a year and after any major incident in the port chain.

Protect

IMO Rev.4: Implement risk control processes and measures to protect computer-based systems: accounts, passwords, multi-factor authentication, segmentation, removable media, training, backups, updates, supply chain policies, audits.

NIST CSF 2.0: Safeguards to manage the organization's cybersecurity risks are used (PR).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	Shared or default passwords on gate kiosks, OCR and crane screens. Vendor remote access stays open all the time. Office IT and operational systems sit on the same network. Nobody had cyber training.	• None	Remove default and shared passwords on the systems that run the gate and the quay, put multi-factor authentication on remote access, and close vendor access that is not in use.
2 Started	Multi-factor authentication protects some remote access and office IT gets its updates, but operational systems are not separated or patched. Training happens now and then.	• VPN settings showing multi-factor authentication • Patch reports for office IT only	Separate operational technology from office IT, give every user a named account, extend the patch policy to OT and train all staff once a year.
3 Defined	Every user has a named account, administrators have a separate one, and remote access asks for a second factor. Operational technology is segmented from office IT, new hardware and software are approved, removable media are controlled, staff are trained every year, and backups and updates follow a written routine.	• Account list with separate admin accounts • Network diagram and firewall rules showing the segmentation • Training attendance records • Patch and backup logs • Removable media policy	Measure the controls: access reviews on a schedule, patch time per severity, a test that the segmentation holds, security clauses in vendor contracts.
4 Managed	The controls are checked, not assumed: access reviews run on a schedule, patch times are tracked, segmentation is tested, critical suppliers sign security clauses and audits check that the measures work.	• Access review records • Patch time per severity, month by month • Penetration or segmentation test summary • Audit report • Vendor contracts with security clauses	Turn test findings and incidents into control changes, and set your security requirements in every software tender.
5 Adaptive	Findings from tests, exercises and incidents change the controls. Security requirements are written into tenders, and connected partners are asked for the same level.	• Security annex of the last software tender • Control changes linked to findings • Connection agreements with partners	Keep it there: review the controls once a year against new threats and new connections.

Detect

IMO Rev.4: Develop, implement and practise activities to detect a cyber incident in a timely manner; maintain a list of relevant threats and actively monitor systems.

NIST CSF 2.0: Possible cybersecurity attacks and compromises are found and analyzed (DE).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	Incidents are found by chance: a frozen screen, a slow TOS, a call from a vendor. Logs are not kept.	• None	Collect the VPN, firewall and TOS logs in one place, keep them, and name the person who looks at alerts.
2 Started	Some systems keep logs for a short time and they are read only after a problem. Antivirus alerts reach the office IT team; operational systems are not watched.	• Log settings of a few systems • Antivirus console	Centralise the logs with a retention period, include operational systems, and have a named person check alerts every working day.
3 Defined	Logs from the TOS, VPN, firewalls, directory and key operational systems are collected centrally. Named people check alerts every day, a list of relevant threats is kept, and staff are trained to recognise an incident.	• List of log sources with retention • Alert handling procedure and rota • Threat list with its last update • Training records	Cover nights and weekends, write detection rules for terminal-specific threats, and measure the time to detect.
4 Managed	Monitoring runs around the clock, in-house or through a service. Rules catch terminal-specific events, such as a new administrator account on the TOS or vendor access outside its window, and the time to detect is measured and reported.	• Detection rule list with test dates • Monthly report with alerts and handling times • Monitoring service contract or rota	Exchange threat information with your port community and the authorities, and tune the rules after every exercise.
5 Adaptive	Threat information is exchanged with the port community and the authorities, the team hunts for threats instead of waiting for alerts, and every incident or exercise improves the rules.	• Information-sharing agreements • Threat hunting reports • Rule changes linked to lessons learned	Keep it there: test the detection once a year with an exercise that simulates a real attack path.

Respond

IMO Rev.4: Develop, implement and practise plans to provide resilience and restore operations impaired by a cyber incident; report incidents within the required time frames and keep records.

NIST CSF 2.0: Actions regarding a detected cybersecurity incident are taken (RS).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	There is no plan. Who decides, who calls the vendors and who reports to the authorities would be worked out on the day.	• None	Write a one-page incident procedure: who decides, who to call, who reports to the authorities, and how the gate keeps running.
2 Started	A contact list and a basic procedure exist but were never practised, and the reporting obligations are unclear.	• Contact list • Procedure document	Write an incident response plan with roles, reporting deadlines and degraded operations, and run a first tabletop exercise.
3 Defined	A written plan sets the roles, who decides, how incidents are reported to the authorities within the required time and how people are informed. Incidents are recorded, staff are trained, and a tabletop exercise took place in the last 12 months.	• Incident response plan with its version date • Incident log • Exercise report • Reporting templates	Practise with operations and vendors, prepare containment steps for the TOS, the gate and operational systems, and measure the time to contain.
4 Managed	Exercises with operations, IT, vendors and management happen at least once a year. Containment steps are ready for the TOS, the gate and operational systems, outside help is arranged in advance, and response times are measured.	• Exercise reports with tracked actions • Containment playbooks • Incident response support agreement • Response time records	Exercise with your chain partners (port authority, shipping lines, hauliers) and agree how you will inform each other.
5 Adaptive	The terminal exercises with its port community, notifications and public messages are coordinated with partners, and lessons learned are shared.	• Joint exercise reports • Communication agreements with partners	Keep it there: change the exercise scenario every year and include a new partner each time.

Recover

IMO Rev.4: Identify and implement measures to restore systems impacted by a cyber incident: recovery strategies for critical systems, training, root cause analysis.

NIST CSF 2.0: Assets and operations affected by a cybersecurity incident are restored (RC).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	Nobody knows where the backups are, or they sit on the same network as the systems. Nobody knows how long a restore would take, and there is no written manual mode for the gate or the yard.	• None	Make an offline or immutable backup of the TOS database and of the key configurations, and write down how the gate works in manual mode.
2 Started	Backups run, but a restore was never tested. People know informally how to work in degraded mode.	• Backup job reports	Test and time a restore of the TOS, and write the recovery priorities and a degraded-mode runbook.
3 Defined	Critical systems have offline or immutable backups, a restore was tested and timed in the last 12 months, the recovery order and the degraded-mode runbook are written, and every incident gets a root cause analysis.	• Restore test report with times • Degraded-mode runbook • Root cause analysis reports	Agree recovery objectives per system with operations, test against them, and run a recovery exercise that includes operational systems and vendors.
4 Managed	Recovery objectives per critical system are agreed with operations, regular restore tests meet them, recovery exercises include vendors, and actions from root cause analyses are followed to closure.	• Recovery objectives table • Test results compared with the objectives • Action tracker	Coordinate recovery with your chain partners, and let recovery lessons shape design and purchasing choices.
5 Adaptive	Recovery is coordinated with the port chain, lessons from incidents and exercises change the architecture, and communication during recovery is planned with partners.	• Joint recovery plans • Architecture changes linked to lessons learned	Keep it there: test a full recovery once a year, including a partner.

Govern

IMO Rev.4: Establish and monitor risk management strategy, expectations and policies; define roles and responsibilities; ensure business continuity and crisis management; designate an accountable person with authority and support.

NIST CSF 2.0: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored (GV).

Level	What it looks like in a terminal	Evidence that proves it	Next step
1 Ad hoc	Nobody is named for cyber. Whoever runs IT handles it when something happens, and management hears about it afterwards, if at all.	• None	Name one accountable person with time and authority, and put cyber on the management meeting agenda.
2 Started	Someone is named but has no budget or authority. A few policies exist as drafts, and management talks about cyber after incidents.	• Nomination note • Draft policies	Have management approve a cyber policy, define the roles, give the accountable person a budget and a regular report.
3 Defined	The accountable person has the authority, support and knowledge the role needs. Management approved the policies, roles are defined, business continuity and crisis management cover cyber, and management receives a regular report.	• Approved policy • Role descriptions • Management meeting minutes • Continuity and crisis plan	Set measurable objectives, have management review them and follow cyber training, and check the measures with audits.
4 Managed	Management reviews objectives and indicators on a schedule, follows cyber training and approves the measures. Audits check that they work, and cyber is part of enterprise risk management and of purchasing.	• Indicator dashboard • Audit reports • Board or management minutes • Training records of managers	Write your target profile and share your expectations with suppliers and partners in the port chain.
5 Adaptive	Cyber is part of the business strategy. The terminal states its target profile to suppliers and partners and takes part in the cyber governance of its port community.	• Strategy document • Supplier requirements • Participation in port community work	Keep it there: review the strategy and the target profile once a year with management.

Sources (public, dated)

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (functional elements Govern, Identify, Protect, Detect, Respond, Recover, paragraph 3.5), 2026-05-28. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

NIST, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (six Functions, Organizational Profiles, Tiers), 2024-02-26. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Directive (EU) 2022/2555 (NIS2), Article 20 (governance) and Article 21 (cybersecurity risk-management measures), 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 grid, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/port-cyber-maturity-grid/ . Generic and anonymised: no terminal, port, client or vendor is named, no statistic. The grid is a self-assessment aid, not an audit, a certification or legal advice.