Maritime Cyber Baseline
Self-Assessment Questions

Version 1.1 October 2022

Introduction

This booklet contains the question set for Maritime Cyber Baseline. It is used for the Level 1 self-assessment and must be completed for all vessels.

In addition, vessels over 500 GRT are required to complete the Level 2 audited stage of assessment to achieve certification, more details of which can be obtained from IASME.

The Maritime Cyber Baseline scheme provides an affordable and practical way for shipping operators and vessel owners to improve their cyber security to reduce the likelihood of a cyber-attack disrupting their day-to-day operations.

The scheme is supported by RINA, the Royal Institution of Naval Architects and enables a path to compliance with the IMO Maritime Cyber Risk Management guidelines.

The scheme is open to vessels of all sizes and classifications, including yachts, commercial, passenger ships and merchant vessels.

Answering the questions

The booklet is intended to help you to understand the questions and take notes on the current setup in your organisation. In order to complete assessment, you must enter your answers via IASME's online assessment platform.

You must answer all questions in order to achieve certification.

Your answers must be approved by a Board level representative, business owner or the equivalent, otherwise certification cannot be awarded.

Need help?

If you need help with understanding the questions, get in contact with IASME on +44 (0)3300 882752 or email info@iasme.co.uk

Alternatively, IASME has a network of Certification Bodies who are skilled information assurance companies who can provide advice on the standards and who can help you make changes to your setup in order to achieve compliance. Visit the IASME website at www.iasme.co.uk to find you nearest Certification Body.

Organisation

D1.1 What is your organisation's official name?

Please provide the full, official name for the organisation being certified. Include the owner or manager of the vessel responsible for the annual document of compliance.

[Notes]

D1.2 What is your organisation's registration number? (If you have one)

This is your organisation's official registration number, as registered with your country's official company, charity, legal or other registration organisation. If you don't have such a number, please leave this blank.

[Notes]

D1.3 What is your organisation's official address?

Please provide the legal registered address for your organisation.

[Notes]

D1.4 What is your organisation's main activity?

Please summarise the main activity of your organisation - if you have multiple activities please provide a brief summary of the most significant ones.

[Notes]

D1.5 What is your website address?

Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer.

[Notes]

D1.6 What is the vessel name?

Please state the registered name - this will appear on your certificate.

[Notes]

D1.7 What is the vessel IMO number?

Please provide vessel IMO number.

[Notes]

D1.8 What is the vessel type?

Please describe the type of vessel.

[Notes]

D1.9 What is the vessel size?

Please specify length (LOA) and Gross Registered tonnage.

[Notes]

D1.10 What is the passenger capacity of the vessel?

Please state the vessel capacity in detail for non-crew members only. (e.g. guests, passengers, etc.).

[Notes]

D1.11 What is the crew capacity of the vessel?

Please state the vessel capacity in detail for crew members only.

[Notes]

D1.12 What is the vessel used for?

Please state if the vessel is used for private, charter or commercial, and to what degree for each.

[Notes]

D1.13 To which flag state is the vessel registered?

Please state the country in which the vessel is listed?

[Notes]

D1.14 Is this application a renewal of an existing certification or is it the first time you have applied for the certification?

This certification requires annual renewal. If you have previously achieved certification please select "Renewal". If you have not previously achieved certification please select "First Time Application".

[Notes]

D1.15 Does the owner or managing company hold a current cyber security certification for their organisation?

Please let us know if your organisation holds a certification such as Cyber Essentials, IASME Governance, ISO 27001, SOC2 or equivalent

[Notes]

D1.16 What is the name and role of the person responsible for managing the security of the systems in this assessment's scope?

Please state the full name and role of the person responsible for managing the IT security of the systems on board the vessel.

[Notes]

Scope Of Assessment

D2.1 Does the scope of this assessment cover your entire vessel (including all information technology (**IT**) and Operational Technology (**OT**) devices, and all on-board networks)?

- Yes
- No

The assessment must cover the whole vessel and all devices within it that are directly or indirectly connected to your networks. Guidance for scoping can be found in the scheme description document.

[Notes]

D2.2 Do you have an asset register that tracks the make, model and operating system version for every device within scope? The asset register **must** track whether a device is categorised as **IT** or **OT**.

- Yes
- No

An asset register should include both physical and informational assets, with assigned owners for each.

[Notes]

D2.3 Please provide a list of all **OT** devices within scope that are designated as "critical systems" as defined by the ISM code.

Please state all systems (including model numbers and versions) classed as "critical systems" within the asset register.

[Notes]

D2.4 Please provide a list of all the networks on the vessel, their function, and details of how each network is segmented from the rest.

Please state each subnet (name and IP range), stating the function and how they are segregated. (e.g. "CREW-NETWORK 10.0.0.1/24 - VLAN through firewall"). You do not need to provide details of external domains or IP addresses. This should include third party systems. Please detail any network segments that are not owned or managed by you and that you have no control over, these third party components will be descoped

[Notes]

D2.5 Please provide a list of all firewalls, switches, routers and security gateways on the vessel, and which networks they support.

Please state the make, model number, internal name and networks they support. (e.g. "Fortinet 40F, crew-firewall, 10.0.0.1, 10.0.0.1/24"). You do not need to provide details of external domains or IP addresses.

[Notes]

D2.6 Please provide a list of all third parties that have remote access or who are provided with physical access to the vessel IT and OT systems. You should include details of the type of access and the purposes for which it is used.

Please list each third party that may require access to the vessel. (e.g. "X-COMPANY. Firewall rule implemented and SSL VPN required, for OT support purposes on an ad-hoc basis").

[Notes]

Firewalls and Security Gateways

D4.1 Does your vessel have firewalls at the boundaries between all internal networks and the internet?

- Yes
- No

This could be hardware or software firewalls.

[Notes]

D4.2 Are these firewalls capable of actively detecting and mitigating attacks through the use of signatures, AI, or other threat detection technologies? Please describe how they do this.

Some firewalls have advanced capabilities that allow them to detect and reduce the impact of attacks. These provide extra protection from internet-based attacks.

[Notes]

D4.3 If your **OT and IT** networks are connected (even occasionally), do you have suitable OT-aware firewalls at the boundaries of all networks containing OT equipment?

- Yes
- No

You must ensure that any firewalls that protect Operational Technology are suitable for the task and have suitable OT-specific protection features enabled.

[Notes]

D4.4 Do you have a map of all data flows between safety critical systems and other on-board **IT and OT** systems?

This should describe how data and information flows between networks. This is usually completed on top of a full network diagram.

[Notes]

D4.5 Do you maintain a list of all firewall rules (inbound and outbound) along with a risk-based justification for each rule?

This includes all hardware and software firewalls.

[Notes]

D4.6 Do you review your firewall rules regularly (at least quarterly)?

- Yes
- No

This includes all hardware and software firewalls. Reviews should be approved by a member of senior management responsible for IT assets.

[Notes]

D4.7 Do you have a process to ensure any firewall rules are disabled in a timely manner when they are no longer required? Describe the process.

Firewall rules should be set as "DENY/DENY" by default. When rules are no longer required they should be returned to their default state. Please describe this process and how it aligns to your firewall reviews.

[Notes]

D4.8 Do you maintain a list of all external services (including cloud services) that interact with the vessel's **OT** assets?

- Yes
- No

It is important to understand which services are interacting with your important OT equipment and by maintaining a list you can then use this to better understand your risks.

[Notes]

D4.9 Are passwords for all firewalls, switches, routers and security gateways at least 10 characters in length, difficult to guess, and have been changed from the default password?

- Yes
- No

Longer passwords make it more difficult for attackers to gain entry to your systems.

[Notes]

D4.10 Do you change the passwords for your firewalls, switches, routers and security gateways when you believe they may have been compromised? How do you achieve this?

Changing passwords when you believe they are compromised improves your security.

[Notes]

D4.11 Do you test simulated attacks to ensure the firewalls are protecting against modern attacks?

- Yes
- No

This could be a full penetration test or a host-based review.

[Notes]

D4.12 Are any of your firewalls configured to allow access to their configuration settings over the internet?

Even if access is permitted on a ad-hoc basis, please describe the reason for this and how it is achieved. (e.g. "Access from our Managed IT Service provider via SSL VPN")..

[Notes]

D4.13 If yes, is there a documented business requirement and risk-based justification for all access?

- Yes
- No

Allowing access to configuration settings presents a risk, so you must be able to understand and justify the provision of such access to allow you to control your risks.

[Notes]

D4.14 If yes, is access to the settings protected by either two-factor authentication or by only allowing trusted IP addresses to access the settings?

- Yes
- No

Both options help ensure that only trusted people are accessing the configuration settings over the internet. You can usually enable these settings in your firewall.

[Notes]

D4.15 Do you have software firewalls enabled on all of your **IT** equipment (including servers, computers and laptops)?

- Yes
- No

Most operating systems have a built-in firewall that can be enabled. In Windows, you can enable firewall in Settings, in macOS you can enable firewall in System Preferences and in Linux try searching for ufw.

[Notes]

D4.16 Are there any services hosted on the vessel which are accessible to the Internet?

- Yes
- No

Some vessels will host services that can be accessed via the internet, such as an email server or a remote access system.

[Notes]

D4.17 If yes, do you ensure all users of these services use a password of at least 10 characters and that your systems do not restrict the length of the password?

- Yes
- No

Longer passwords make it more difficult for attackers to gain entry to your systems.

[Notes]

D4.18 If yes, do you ensure that you change passwords if you believe that they have been compromised?

- Yes
- No

This includes all hardware and software firewalls. Reviews should be approved by a member of senior management responsible for IT assets.

[Notes]

D4.19 If yes, are your services set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?

- Yes
- No

Lockouts and timeouts make it more difficult for attackers to gain access to your system.

[Notes]

Secure Configuration

D5.1 Where you are able to do so, have you removed or disabled all the software that you do not use on all **IT and OT** devices (including servers, computers, laptops, tablets and mobile phones)? Describe how you achieve this.

Unused software presents security risks because it is often not updated and presents a potential route for attack. You should actively choose which software should be installed on each device.

[Notes]

D5.2 Have you ensured that all your **IT and OT** devices only contain necessary user accounts that are regularly used for legitimate business purposes?

- Yes
- No

Removing unnecessary user accounts improves the security of your devices.

[Notes]

D5.3 Do you have a password policy that applies to all users of vessel systems that provides guidance on how to choose non-guessable passwords, password reuse, which passwords may be written down, where they can be stored, and use of password managers?

Please describe your password policy regarding this. Please also provide the software and version of your approved password manager(s) if applicable.

[Notes]

D5.4 Do you distribute the password policy to all users of vessel systems when they are first provided access to the vessel?

- Yes
- No

Upon first login, all users should be prompted to change and set a secure password.

[Notes]

D5.5 Do you change the password for **IT and OT** devices when you believe the password may have been compromised? How do you achieve this?

Please describe your password policy regarding this. Passwords should be regularly checked for compromise and be reset when there is sufficient reason to.

[Notes]

D5.6 Do you ensure all your wifi networks (excluding guest) have strong encryption enabled and use non-guessable passwords?

- Yes
- No

You should ensure that wifi passwords are at least 10 characters and use a combination of numbers, letters and symbols that are difficult to guess. You may wish to regularly change wifi passwords if there is a risk that previous guests and crew may continue to use your networks (such as when docked at a regular location.

[Notes]

D5.7 Have you ensured that all wifi network names (SSIDs) are configured so that they do not identify a vessel sensitive system or a person?

- Yes
- No

Vessels often name their wifi networks after the name of the vessel or the owner. This makes it much easier for hackers, criminals and other threats to identify which network to attack. It also increases the risk that the mobile devices of vessel owners and other staff can be identified and targeted.

[Notes]

D5.8 Have you enabled two-factor authentication for all local administrative accounts on **IT and OT** devices and all administrative accounts on cloud services?

- Yes
- No

Teo-factor authentication improves the security of administrator accounts and should be used wherever possible.

[Notes]

D5.9 If no, is this because two-factor authentication is not available for some or all of your devices or services? List the devices or services that do not allow two-factor authentication.

Please state all makes, models, and versions as applicable. Please state the reason why MFA has not been configured for each device or service.

[Notes]

D5.10 Do you provide guidance and have a set policy for staff on the secure use of removable media with vessel systems? Removable media includes USB memory sticks and other USB devices such as mobile phones. Please provide details of the policy.

Removable media can be a method by which viruses such as ransomware can be transferred to systems on your vessel. It also presents a risk of data loss because removable media can store a large amount of data in a small device which is easily lost.

[Notes]

Managing Vulnerabilities

D6.1 Are all **operating systems** and **firmware** on your **IT** devices supported by a supplier that produces regular fixes for any security problems?

- Yes
- No

It is vital that all operating systems are supported by the manufacturer and that security updates are being provided by the manufacturer to you on a regular basis. You can use open source software as long as regular security updates are being provided to you by the community.

[Notes]

D6.2 Are all **applications** on your **IT** devices supported by a supplier that produces regular fixes for any security problems?

- Yes
- No

It is important to minimise the amount of information that an attacker can learn about the device via the network - this makes it harder for the attacker to understand the device's specific vulnerabilities and exploit them.

[Notes]

D6.3 Are all high-risk or critical security updates for **operating systems, firmware and applications** on your **IT** devices installed or scheduled for deployment, within 30 days of release? Describe how you achieve this.

High-risk or critical security updates are those that the manufacturer describes as high-risk or critical in the release notes for the update. If the manufacturer doesn't provide a description, high-risk or critical means any security updates that address vulnerabilities rated 7 or higher on the NIST CVSS vulnerability scoring methodology (https://nvd.nist.gov/vuln-metrics.

[Notes]

D6.4 Are all **operating systems** and **firmware** on your **OT** devices supported by a supplier that produces regular fixes for any security problems?

- Yes
- No

It is vital that all operating systems are supported by the manufacturer and that security updates are being provided by the manufacturer to you on a regular basis.

[Notes]

D6.5 Are all **applications** on your **OT** devices supported by a supplier that produces regular fixes for any security problems?

- Yes
- No

It is vital that all applications are supported by the manufacturer and that security updates are being provided by the manufacturer to you on a regular basis.

[Notes]

D6.6 Are all high-risk or critical security updates for **operating systems, firmware and applications** on your **OT** devices installed, or scheduled for deployment, within 30 days of release? Describe how you achieve this.

- Yes
- No

High-risk or critical security updates are those that the manufacturer describes as high-risk or critical in the release notes for the update. If the manufacturer doesn't provide a description, high-risk or critical means any security updates that address vulnerabilities rated 7 or higher on the NIST CVSS vulnerability scoring methodology (https://nvd.nist.gov/vuln-metrics).

[Notes]

D6.7 If no, please provide details of which **OT** systems have outstanding critical vulnerabilities, the reason why security updates have not been installed and confirmation of senior management knowledge and acceptance of the vulnerability.

Please list each critical vulnerability on OT systems and applications. Please state the business justification for not remediating these, the name and role of the member of senior management who approved this decision, when it was identified, and when it was last reviewed.

[Notes]

D6.8 Have you conducted a vulnerability assessment within the last 12 months, in order to identify any missing security updates? Describe how you achieve this.

Please provide details of the frequency and scope of the assessments (which systems and networks are included) and the process you follow.

[Notes]

Access Control

D7.1 Are crew only provided with user accounts after a process has been followed to approve their creation? Describe the process.

Please describe how user access is provisioned. This should include prompting the user to change their password upon the initial login and ensuring that segregation of duties and the principle of least privilege is followed.

[Notes]

D7.2 Do you ensure that crew have only the privileges that they need to do their current job? How do you achieve this?

It is important that crew only have the minimal access needed to carry out their current job, this minimises the risk of unauthorised changes being made to systems.

[Notes]

D7.3 Have you deleted, or disabled, all user accounts for crew who have departed the organisation? Please describe the process.

Accounts that are no longer required should be disabled and then deleted. This includes those users who are going on rotation and do not require access to the vessel systems.

[Notes]

D7.4 Have you documented any **IT or OT** devices that are accessible with a shared password?

It is best practice to not allow shared accounts or passwords. If applicable, please describe where this is the case, including the business reason for allowing it, and specify the member or senior management who has approved this.

[Notes]

D7.5 Do you have a formal process for giving someone access to systems at an “administrator” level? Describe the process.

You must have a formal, written-down process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.

[Notes]

D7.6 Do you review who should have administrative access on a regular basis?

- Yes
- No

You must review the list of people with administrator access regularly. Depending on your organisation, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.

[Notes]

Malware Protection

D8.1 Are all of your **IT devices** protected from malware by either A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or C - another method.

- A – Anti-Malware Software
- B – Limiting Installation of Applications to an Approved Set
- C – Another Method

All IT systems must be protected by one of either three options.

[Notes]

D8.2 (A) Where you have anti-malware software installed on your IT devices, is it set to update daily and scan files automatically upon access?

- Yes
- No

This only applies to systems with anti-malware software installed.

[Notes]

D8.3 (A) Where you have anti-malware software installed on your IT devices, is it set to scan web pages you visit and warn you about accessing malicious websites?

- Yes
- No

Most anti-virus software are configured to do this.

[Notes]

D8.4 (B) Where you use an app-store or application signing on your IT devices, are users restricted from installing unsigned applications?

- Yes
- No

This only applies to systems with application signing or systems that use an app-store (this includes an approved Self-Service Software Centre).

[Notes]

D8.5 (B) Where you use an app-store or application signing on your IT devices, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?

- Yes
- No

You must create a list of approved applications and ensure users only install these applications on their devices.

[Notes]

D8.6 (C) Where you use another method on your IT devices, please provide details of the method used and how it provides suitable protection against malware for your risk environment.

Please describe the technical controls involved in detail and your justification for their usage.

[Notes]

D8.7 Are all of your **OT devices** protected from malware by either A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or C - another method.

- A – Anti-Malware Software
- B – Limiting Installation of Applications to an Approved Set
- C – Another Method

All OT systems must be protected by one of either three options. This applies to OT systems that are accessed on an ad-hoc basis by support providers over the internet.

[Notes]

D8.8 If no to above, please provide details of which OT devices are not protected from malware, the reason why no malware protection is in place and confirmation of senior management knowledge and acceptance of the risks involved.

Please explain the process of accepting this risk, who approves this risk, when it was identified, and when it was last reviewed.

[Notes]

D8.9 (A) Where you have anti-malware software installed on your OT devices, is it set to update daily and scan files automatically upon access?

- Yes
- No

This only applies to systems with anti-malware software installed.

[Notes]

D8.10 (A) Where you have anti-malware software installed on your OT devices, is it set to scan web pages you visit and warn you about accessing malicious websites?

- Yes
- No

Most anti-virus software are configured to do this.

[Notes]

D8.11 (B) Where you use an app-store or application signing on your OT devices, are users restricted from installing unsigned applications?

- Yes
- No

This only applies to systems with application signing or systems that use an app-store (this includes an approved Self-Service Software Centre).

[Notes]

D8.12 (B) Where you use an app-store or application signing on your OT devices, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?

- Yes
- No

You must create a list of approved applications and ensure users only install these applications on their devices.

[Notes]

D8.13 (C) Where you use another method on your OT devices, please provide details of the method used and how it provides suitable protection against malware for your risk environment.

Please describe the technical controls involved in detail and your justification for their usage.

[Notes]

Secure Business Operations

D9.1 Have you carried out a risk assessment that covers information and cyber risks to your vessel?

- Yes
- No

Conducting a risk assessment is an important step towards improving your security. It is a key element of the IMO requirements around cyber security for vessels. IASME can provide a risk assessment template to assist this process.

[Notes]

D9.2 Are changes to **IT and OT** device configuration reviewed and approved by an authorised person, and are users disallowed from making changes without approval? Describe the approval process.

Changes to systems should be approved by a suitable person with a decision-making role in the organisation. Users should not be able to make changes without approval. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.

[Notes]

D9.3 Are all **IT and OT** devices configured to the manufacturer's recommended build and security standards? Describe how you achieve this.

Please describe the manufacturer's recommendations for each system in scope and how you meet them.

[Notes]

D9.4 Are backups of data and configuration of **IT and OT** devices performed regularly, maintained, and tested?

- Yes
- No

It is important that backups are stored in a safe location, ideally a different physical location from the source of the data. You should carry out a regular test of the backups to ensure they will be usable if a cyber incident affects the original device.

[Notes]

D9.5 Do you keep the logs created by your anti-malware systems and firewalls stored securely to allow analysis in the event of an incident?

- Yes
- No

Logs are important to allow investigation of any cyber incidents and to prevent their reoccurrence.

[Notes]

D9.6 Do you regularly review the logs you receive to identify any suspicious activity? How do you achieve this?

Regularly reviewing logs means you are more likely to spot suspicious activity and be able to prevent further incidents.

[Notes]

D9.7 Do you regularly review the activities of third-parties who have access to your **IT and OT** devices to identify any suspicious actions?

- Yes
- No

Monitoring the activities of third-parties helps you to detect any cyber incidents that may be occurring within your supply chain.

[Notes]

D9.8 Do you maintain a baseline secure configuration for all **IT and OT** devices which can be used when setting up any new or replacement devices? How you achieve this?

It is best practice to configure a "gold build", which is a secure standard setup which will be applied to all devices of a similar type. Consider your processes for ensuring that changes to systems do not mean the security provided by this baseline configuration standard is affected.

[Notes]

D9.9 Do all new and existing crew receive basic training in cyber security before being given access to **IT and OT** devices?

- Yes
- No

Basic cyber training helps ensure that crews are informed and able to act appropriately to reduce cyber threats.

[Notes]

D9.10 Do you provide ongoing training for crew in cyber security? Please provide details of the type of training and the topics covered.

Ongoing training ensures that crew's knowledge of cyber remains current and is an opportunity to highlight any particular threats to the vessel.

[Notes]

D9.11 Is there a documented incident response plan that is executed in response to cyber security incidents to reduce their impact on the organisation? Please describe the plan.

A response plan provides helpful guidance on how to deal with an incident during what will be a stressful time. You must ensure that all relevant employees are aware of the plan and how to follow it. This could be included in your crew training.

[Notes]

D9.12 Is there a documented process to restore systems to a trusted configuration after a security incident has occurred?

- Yes
- No

Having a clear process to restore to a trusted configuration ensures the secure resolution of any incidents and rapid return to normal operation.

[Notes]