threatscene
MARINE

The **MARINE** Cyber Security Framework

Version: 1.0

https://marine.threatscene.com

marine@threatscene.com

While the MARINE Cyber Security Framework provides detailed guidance to enhance Maritime organisations cyber security posture, it does not guarantee immunity and complete protection from all security threats. ThreatScene Greece MAE (ThreatScene Marine) is not liable for any implementation errors, misconfigurations, or other user actions during the adoption process. Additionally, users must acknowledge that despite thorough adherence to the framework's controls, residual risks and vulnerabilities may persist, and compromise or incidents could still occur. It is therefore recommended that organisations continually assess, monitor, and update their security measures to continuously adapt to evolving cyber risks.

ThreatScene MARINE

MARINE Cyber Security Framework Introduction

The **MARINE Cyber Security Framework** is a comprehensive set of security guidelines and standards, specifically designed to address the distinct security challenges faced by the maritime industry. MARINE covers the fundamental aspects of cyber security and demonstrates compliance with other applicable standards such as NIS2, IMO, and GDPR.

With growing reliance on digitalisation, the risks applicable to shipping companies are increasing. Cyber threats can significantly disrupt operations, compromise safety, result in legislative non-compliance, and ultimately lead to significant financial losses.

MARINE offers a structured approach to building robust cyber defences and managing compliance in a standardised way, ensuring that maritime organisations can operate securely and efficiently, and creates confidence in the organisation's security posture.

Scope and Applicability

The MARINE framework is intended for shipping companies, ports, and maritime service providers, providing a standardised approach to protect information technology systems and the data they process.

MARINE aligns with emerging regulatory frameworks like **NIS2** (Network and Information Security Directive 2), and the **IMO** Cyber Risk Standard (International Maritime Organisation), ensuring maritime organisations meet evolving cyber security requirements, and that there is consistency between applicable frameworks.

The Core Categories within the MARINE Cyber Security Framework

M

Monitoring Threats - Proactive and continuous monitoring of systems to detect, analyse, and respond to potential cyber threats in real-time.

A

Access Control (A&A) - Security enforcing mechanisms to only grant access to Authenticated and Authorised users (either human or system), whilst applying principles of least privilege.

R

Regulatory Compliance and Risk Management - Aligning with international regulations and industry standards, with demonstratable compliance that maritime operations meet legal and contractual requirements.

I

Incident Response Planning - Establishing clear protocols to quickly and effectively respond to and recover from cyber incidents, minimising impact on operations.

N

Network Security - Implementing security controls to protect internal and external network communications, including onboard systems and onshore infrastructure.

E

Education - Continuous training and awareness programs to equip maritime professionals with the knowledge to recognise and mitigate cyber risks.

To assist companies in preparing for the **MARINE Cyber Security Framework**, we have developed a self-assessment platform. Companies can register and complete the assessment to benchmark themselves against others in the maritime industry and receive a comprehensive report highlighting areas for improvement.

The platform is available at: `https://marine.threatscene.com`

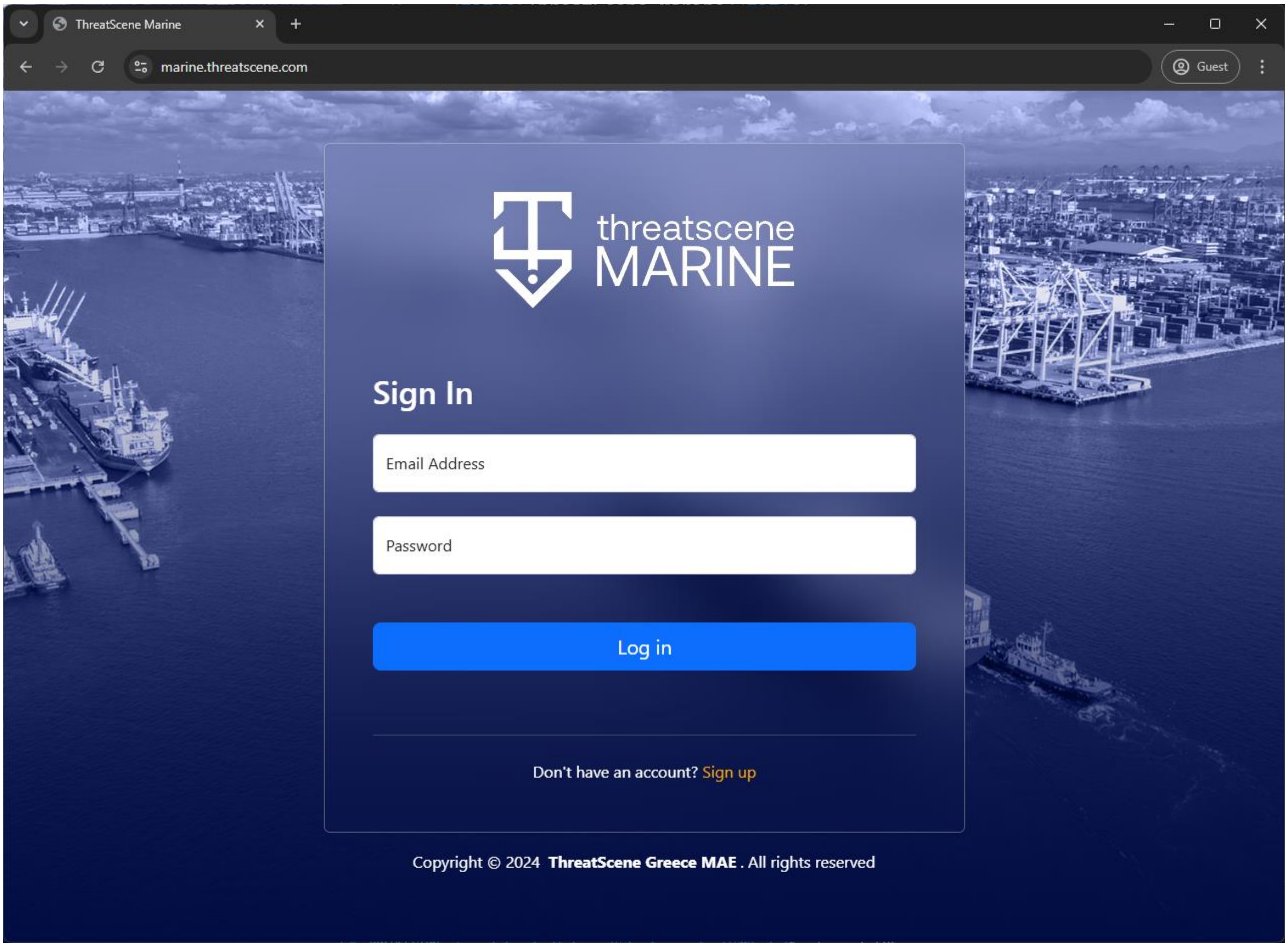


Figure 1: The ThreatScene Marine Platform

MARINE Cyber Security Framework Contents

MARINE includes the following six core Categories and their pertinent Security Controls, which cover the core fundamental concepts within cyber security.

This section introduces the Categories and their corresponding Security Controls, however there is a deep-dive section that includes further detail and implementation actions within the ***MARINE Cyber Security Framework Handbook*** chapter.

Monitoring Threats

M1. **Security Information and Event Management (SIEM)**: Implement SIEM tools to aggregate and analyse security data to understand the organisations systems and network.

M2. **User Activity Monitoring**: Monitor user activities to detect insider threats or potential malicious activity, with a particular focus on privileged users or administrators.

M3. **Vulnerability Scanning**: Regularly scan for vulnerabilities in systems and applications.

M4. **Intrusion Detection Systems (IDS)**: Deploy IDS to detect suspicious activity.

M5. **Endpoint Detection and Response (EDR)**: Use EDR solutions to monitor and respond to threats at endpoints like laptops, desktops, and mobile devices in real time.

M6. **Threat Intelligence Feeds**: Subscribe to threat intelligence services for real-time updates on emerging threats to ensure a proactive approach to security vulnerabilities.

M7. **Log Management**: Establish a centralised logging mechanism for all systems and detect and understand anomalies – this should integrate with the IDS and EDR systems.

M8. **Regular Security Audits**: Conduct regular audits and assessments of security controls.

M9. **Third-Party Risk Monitoring**: Continuously monitor the cyber security posture of third-party suppliers and service providers, as they may introduce vulnerabilities into your system.

Access Control (A&A)

A1. **Strong and Validated Authentication**: Implement strong authentication mechanisms for users and systems, such as complex passwords with multi-factor authentication (MFA) and biometric validation for users. System to System authentication should use strong mechanisms such as Secure Tokens or PKI Certificates.

A2. **Access Control Policies to enforce Authorisation**: Develop and maintain formal access control policies, enforcing strong authorisation decisions made by a centralised mechanism.

A3. **Password Management**: Enforce strong password policies and regular password changes for both users and systems.

A4. **Privileged Account Management**: Monitor and manage privileged users and administrators closely, ensuring regular reviews if personnel still require the high level of privilege.

A5. **Access Based on Least Privilege**: Ensure all access is granted based on the principle of least privilege, providing the minimal necessary permissions to perform tasks. This should apply to both user and system access.

A6. **Account Provisioning and Deprovisioning**: Ensure timely provisioning and deprovisioning of accounts, which are automatically triggered on personnel joiner, mover, or leaver activity.

A7. **Access Reviews**: Regularly review user access rights.

A8. **Remote Access Security**: Ensure secure methods for remote access to critical systems.

Regulatory Compliance and Risk Management

R1. **Risk Management**: Ensure that cyber security risks are identified via threat modelling, architecture reviews, or technical security tests, and are then risk managed through life.

R2. **Regulatory Frameworks**: Demonstrate documented compliance with relevant regulations and standards, such as NIS2, IMO, NIST CSF, and GDPR.

R3. **Compliance Audits**: Conduct periodic audits to ensure compliance with regulations.

R4. **Privacy Impact Assessments (PIAs)**: For any new system or technology being introduced, conduct PIAs to ensure it complies with privacy regulations like GDPR. This can help in minimising risks related to data processing.

R5. **Document Retention Policies**: Establish policies for retaining compliance-related documents in a secure repository.

R6. **Data Protection Policies**: Implement data protection policies and controls compliant with regulations.

R7. **Data Breach Notification Procedures**: Establish procedures for notifying stakeholders of data breaches, which is a key requirement of GDPR.

R8. **Incident Reporting Requirements**: Adhere to incident reporting requirements set forth by regulators.

R9. **Third-Party Management**: Assess and manage risks associated with third-party vendors and suppliers.

R10. **Continuous Monitoring for Compliance**: Set up automated systems to continuously monitor and report on compliance with regulatory frameworks and risk management measures, ensuring real-time updates and swift mitigation of any non-compliance issues.

Incident Response Planning

I1. **Incident Response Plan**: Develop and maintain a comprehensive incident response and reporting plan.

I2. **Incident Categorisation**: Establish a categorisation scheme to categorise incidents to enable appropriate responses.

I3. **Response Team Roles**: Define roles and responsibilities for the incident response team.

I4. **Communication Plan**: Create a communication plan for stakeholders during incidents.

I5. **Intrusion Detection Tools**: Use automated tools to prepare responses for intrusion detection.

I6. **Incident Response Training**: Provide training for personnel on incident response procedures, such as tabletop exercises.

I7. **Backup, Resilience, and Disaster Recovery**: Define and regularly test backup and recovery procedures.

I8. **Post-Incident Review**: Conduct reviews after incidents to improve the efficiency and speed of future responses.

I9. **Forensic Analysis**: Ensure that a secure forensic environment and process is established to ensure that logs, information, and images can be analysed safely.

I10. **Testing Incident Response Plans**: Regularly test and update incident response plans to align with best practice and emerging threats.

Network Security

N1. **Firewalls**: Implement firewalls to protect network boundaries and manage ingress and egress of network traffic.

N2. **Intrusion Prevention Systems (IPS):** Deploy IPS to prevent malicious activities.

N3. **Network Segmentation**: Use segmentation to isolate critical systems and protect all systems that are not user facing.

N4. **Secure Configuration**: Establish secure configurations for all network devices and ensure appropriate documentation is maintained.

N5. **Encryption of Data in Transit:** Use encryption for data transmitted over the network using next-generation encryption algorithms.

N6. **Encryption of Data at Rest**: Ensure all sensitive data stored on devices, servers, and databases is encrypted. This protects the confidentiality even if devices or systems are compromised.

N7. **Virtual Private Networks (VPN)**: Use VPNs for secure and encrypted remote access.

N8. **Penetration Testing**: Identifying vulnerabilities in the network and associated systems through technical security testing.

N9. **Patch Management**: Regularly update and patch system and network devices.

N10. **Data Localisation and Network Boundaries**: Ensure compliance with NIS2's requirements on data storage and network boundaries, specifically protecting data crossing EU borders and ensuring networks comply with EU standards.

Education

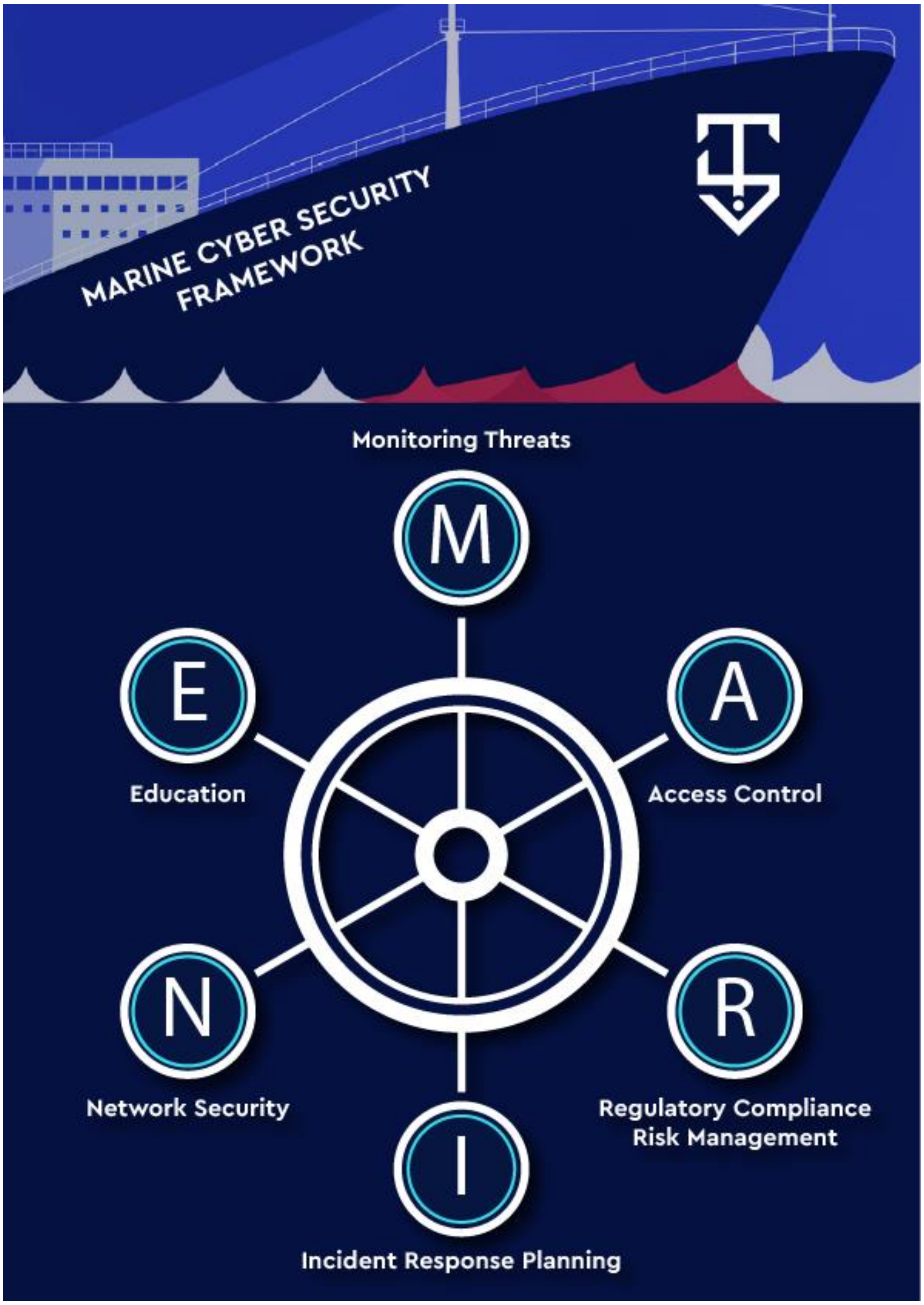
E1. **Security Awareness Training**: Provide ongoing security awareness training for all employees, to raise awareness and understanding of cyber security policies and best practice.

E2. **Phishing Simulations**: Conduct phishing simulations to test employee responses and security awareness.

E3. **Incident Response Drills**: Regularly conduct drills to test incident response readiness, including procedures such as backup and recovery.

E4. **Role-Specific Training**: Offer role-specific security training for sensitive positions such as privileged users and administrators.

E5. **Continuous Learning Opportunities**: Encourage continuous professional development in cyber security, including any applicable certifications.


MARINE CYBER SECURITY FRAMEWORK
Monitoring Threats
M
E
Education
A
Access Control
N
Network Security
R
Regulatory Compliance Risk Management
I
Incident Response Planning

References to Regulatory Frameworks

For demonstratable compliance with other relevant Regulatory and industry recognised Frameworks, MARINE is aligned against NIS2, IMO Resolution MSC.428(98), NIST CSF, and GDPR.

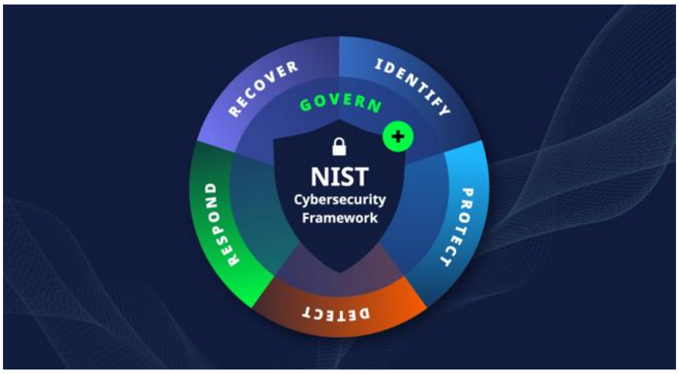
MARINE has been developed in a way to ensure that achieving compliance will enable your organisation to provide similar evidence for demonstrated compliance with the respective frameworks.

- ✓ **NIS2**: Directive on the security of network and information systems within the EU, focusing on resilience and incident response in essential services. As a member state of the EU, Greece is obligated to introduce NIS2 compliance, and under Annexe I Water Transport, this includes the Maritime industry within the scope.

- ✓ **IMO Resolution MSC.428(98)**: The International Maritime Organisation established cyber security guidelines for the maritime industry to ensure that shipping companies and their assets are protected against cyber threats.

- ✓ **NIST CSF**: National Institute of Standards and Technology Cyber Security Framework, which provides a comprehensive approach to managing cyber security risks.

- ✓ **GDPR**: General Data Protection Regulation is an EU law introduced in 2018 that governs data privacy and protection, giving individuals control over their personal data and imposing strict requirements on how organisations collect, store, and process it, and also robust requirements on reporting breaches and incidents.



Critical Assets within Maritime

Several systems, including the underlying applications, software, and infrastructure within the maritime industry are susceptible to cyber threats and must be protected, including:

- **Passenger Services**: Systems managing passenger information and services, where breaches can lead to privacy violations.
- **Public Networks**: Networks accessible by passengers and crew, which can be entry points for cyber threats.
- **Access Control Systems**: Security systems that manage entry and exit points, crucial for preventing unauthorised access.
- **Administrative Systems**: Software used for ship administration and crew welfare, important for overall operational management.
- **Fleet Management and Remote Monitoring Systems**: Systems that provide centralised data collection and management capabilities, usually operated onshore to monitor vessel conditions, efficiency, and coordination.
- **Communication Systems**: Both internal and external communication systems and their respective networks, for transmission of information and telemetry.
- **Navigation Systems**: Systems including GPS, Automatic Identification System (AIS), radar, and Electronic Chart Display and Information System (ECDIS).
- **Telemetry Systems**: Telemetry data is critical for navigation, maintenance, and operational efficiency – it is used for real-time data collection and diagnostics across various onboard functions.
- **Bridge Systems**: These include navigation and control systems essential for the safe operation of vessels.
- **Cargo Handling Systems**: Equipment and software used for managing cargo, which, if compromised, can disrupt logistics and supply chains.
- **Propulsion and Machinery Management**: Systems that control ship engines and machinery, which is vital for maintaining operational capabilities.

Threat Actors

The potential threat actors who may target maritime operations include:

- **Nation State Actors**: Who may conduct sophisticated and targeted attacks with strategic or geopolitical objectives that are state financed.
- **Criminals and Organised Crime**: Who seek financial gain through cyber attack, such as ransomware or data theft.
- **Insider Threats**: Who may intentionally or accidentally cause harm through negligence or lack of awareness.
- **Activists**: Who may target specific ships or companies for political or social reasons.

MARINE Cyber Security Framework Handbook

The following section will provide a deep-dive into the core Categories within MARINE, the justification behind the Security Controls, and applicable implementation actions.

Monitoring Threats

Monitoring is a foundational aspect of any cyber security strategy, particularly in the maritime sector, where both onboard and onshore systems must remain secure. The purpose of monitoring is to detect, analyse, and respond to threats in real-time, ensuring the ongoing security and operational integrity of vessels, shipping company infrastructure, and related digital systems.

M1. Security Information and Event Management (SIEM)

SIEM systems pull security logs from various sources such as firewalls, servers, and network devices. It centralises the data and uses predefined rules to detect anomalous or suspicious activity. For example, it might trigger an alert if it notices multiple failed login attempts followed by a successful login from an unrecognised IP address.

Implementation Actions:

- □ Implement a real-time SIEM solution (aligned with NIS2) that can be adapted to specific operational technologies (for IMO) and can track data processing activities (for GDPR).
- □ Identify key systems to be monitored (e.g., navigation, communication, engine control systems).
- □ Configure information sources to forward logs to the SIEM.
- □ Define correlation rules tailored to shipping-specific threats (e.g., abnormal access to control systems from unrecognised IPs).
- □ Clearly define and assign appropriate roles and personnel to the organisations SOC (Security Operations Centre) and CISRT teams (Cyber Security Incident Response Teams) to understand and analyse the security logs.
- □ Ensure there is a dedicated team to regularly review SIEM alerts and incidents to refine detection mechanisms.

M2. User Activity Monitoring

Implement monitoring of user activities, focusing on privileged users and administrators to detect insider threats, compromised accounts, or unauthorised actions. User activity monitoring helps identify anomalous behaviour that may compromise the integrity of the ship's network or control systems.

In shipping, this could mean logging who accesses the ship's ECDIS (Electronic Chart Display and Information System) and what activity is taken, when maintenance commands are executed, or if an administrator accesses the satellite communication system. For instance, if an engineer logs into a control system during out of hours, this could trigger an alert, prompting further investigation.

Implementation Actions:

- □ Set up a logging solution that tracks user actions, especially those of privileged users, to proactively monitor for suspicious activity.
- □ Define key actions that should trigger alerts (e.g., unauthorised access to control systems, and unusual access times).
- □ Set up alerting for activities involving sensitive data, such as unauthorised file transfers or access attempts to enable data loss prevention (DLP) principles.
- □ Regularly review logs for suspicious activity and adjust access controls if necessary.
- □ Provide training to crew members on the importance of logging and ensuring that unauthorised access is reported immediately to raise awareness.

M3. Vulnerability Scanning

Regularly scan the ship's networks and systems to identify vulnerabilities before they can be exploited by malicious actors. This includes scanning both onshore and onboard systems to detect outdated software, misconfigurations, or missing patches.

Vulnerability scanning involves using automated tools to check systems for known vulnerabilities within the CVE Database. These tools will scan the entire IT infrastructure - including servers, onboard systems, communication networks, and device endpoints - for security vulnerabilities with known exploits.

Implementation Actions:

- □ Schedule periodic scans of both onboard and onshore systems using a vulnerability scanner (i.e., every 90 days, or when a change is deployed into Production.
- □ Ensure that critical systems (e.g., telemetry, navigation, engine control, communication) are included in the scans.
- □ Review scan results and prioritise remediating critical vulnerabilities that could impact operational safety.
- □ Keep systems up to date by regularly applying security patches at a regular cadence, i.e. following Microsoft's Patch Tuesday.

M4. Intrusion Detection Systems (IDS)

Deploy IDS to monitor and detect unauthorised or suspicious activity within the network. IDS tools help detect early signs of an attack, such as malicious traffic or unauthorised access attempts, allowing swift responses to potential breaches.

For instance, in a shipping environment, an IDS could detect an unauthorised attempt to access the ship's control communication and telemetry systems, or a series of failed login attempts from an unrecognised IP address.

Implementation Actions:

- □ Deploy an IDS to monitor critical network segments, including the ship's control network and onshore systems.
- □ Configure the IDS to recognise shipping-specific threats, such as abnormal access to vessel control systems.
- □ Set up an alerting system to notify the security team in the event of a detected anomaly.
- □ Ensure personnel within the SOC / CISRT Teams regularly review IDS logs and alerts to identify patterns that may indicate a sophisticated attack.
- □ Ensure that the IDS system is configured securely, and has sufficient A&A controls and monitoring applied, as it will be an attractive target for any adversaries to disable.

M5. Endpoint Detection and Response (EDR)

Implement EDR solutions to monitor and respond to threats at endpoints, such as crew laptops, onboard control terminals, and mobile devices. EDR tools enable real-time monitoring, detection, and remediation of endpoint threats like malware, ransomware, or unauthorised access attempts.

In the shipping context, this could involve detecting a compromised off-duty crew laptop that's connected to the ship's network out of hours, or identifying malware trying to propagate from an onboard system to an onshore server.

Implementation Actions:

- □ Install EDR agents on all critical endpoints, including crew devices and onboard systems.
- □ Configure EDR tools to automatically isolate endpoints if suspicious activity is detected (e.g., malware or unauthorised access attempts).
- □ Ensure personnel within the SOC / CISRT Teams regularly review endpoint logs and alerts to identify potential threats, and improve endpoint defences.

M6. Threat Intelligence Feeds

Subscribe to threat intelligence feeds to receive real-time updates on emerging cyber threats. These services provide critical information about the latest vulnerabilities, attack vectors, and threat actors, helping to keep your security defences up-to-date and proactive.

These feeds help organisations stay ahead of potential attacks by updating security tools, adjusting defence strategies, and blocking malicious IP addresses or domains known to be associated with cybercriminals.

Implementation Actions:

- □ Subscribe to relevant maritime-specific and general cyber security threat intelligence services.
- □ Integrate threat intelligence feeds with security systems like SIEM (Security Information and Event Management tool) and firewalls for automatic blocking of known threats.
- □ Review threat intelligence updates regularly and incorporate new information into risk assessments and response plans.

M7. Log Management

Implement a centralised logging mechanism to collect, store, and analyse logs from all systems across the organisation, enabling detection of anomalies and aiding in incident investigations.

Centralised logging ensures that any suspicious activity or deviation from normal operations is recorded and flagged for further investigation.

Implementation Actions:

- □ Set up a central log server to collect and store logs from all systems and the network, including both onboard and onshore systems.
- □ Ensure sensitive logs are encrypted and stored for an appropriate period as defined by regulations, allowing for forensic investigations post-incident.
- □ Regularly review and audit logs to detect security incidents and assess system health.

M8. Regular Security Audits

Conduct regular security audits to assess the effectiveness of existing security controls, identify vulnerabilities, and ensure compliance with applicable cyber security regulations such as NIS2, IMO MSC.428(98), and GDPR.

Audits typically review aspects such as access control, vulnerability management, incident response, and physical security of critical systems. For maritime operations, this might involve auditing the security of onboard networks, assuring the data integrity of telemetry, the effectiveness of encryption on communication channels, the robustness of the ship's access control systems, and how personnel and customer PII is managed and processed.

Implementation Actions:

□ Schedule regular security audits to evaluate all aspects of your cyber security framework.

□ Engage third-party auditors who specialise in maritime cyber security to conduct objective reviews of your systems.

□ Address any vulnerabilities or compliance issues identified during the audit and update security controls accordingly.

□ Document all audit findings and corrective actions to ensure a clear audit trail and for future regulatory inspections, enabling a compliance improvement roadmap over time.

M9. Third-Party Risk Monitoring

Continuously monitor the cyber security posture of third-party suppliers and service providers to ensure they do not introduce vulnerabilities into your network or operations. Supply chain security is a critical area of the security posture of your organisation, as any compromise of an interconnected or dependant partner can result in lateral movement by attackers that can impact your systems.

This includes reviewing their security policies, conducting security assessments, and ensuring they adhere to industry best practices. In the maritime context, third-party risk could arise from poorly secured software updates delivered by a vendor, unsecured connections to external ports, or third-party personnel accessing critical systems onboard the vessel.

Implementation Actions:

□ Assess all third-party suppliers and service providers for their cyber security practices before agreeing service level agreements and contracts.

□ Require third parties to comply with your organisation’s cyber security policies (such as MARINE), particularly in handling sensitive data or accessing critical systems.

□ Regularly audit third-party services and systems to ensure they are secure and compliant with industry regulations.

□ Ensure contracts include clauses that mandate security incident reporting, vulnerability management, and ongoing cyber security training for third-party personnel.

Access Control (A&A)

Access Control (Authentication & Authorisation) is a critical component of cybersecurity, ensuring that only authorised users or systems can access sensitive systems, networks, and information. By enforcing strict access control mechanisms, organisations can limit the potential for unauthorised access or misuse, thus protecting vital operational systems from both internal and external threats.

A1. Strong and Validated Authentication

Implement secure authentication mechanisms for both users and systems, ensuring that access to critical systems is restricted only to authorised individuals and devices, significantly reducing the risk of unauthorised access or cyber attacks.

For users, authentication can be achieved by enforcing multi-factor authentication (MFA), which combines something the user knows (password), with something they have (a smartphone or token), or something they are (biometric data). System-to-system authentication should use advanced mechanisms like Secure Tokens or Public Key Infrastructure (PKI) Certificates, which validate the identity of communicating systems and enforce encrypted communications.

For example, crew members accessing sensitive onboard systems such as the ECDIS (Electronic Chart Display and Information System) could be required to use biometric authentication along with a password, while telemetry communication systems between vessel navigation systems and onshore control could be secured using encryption.

Implementation Actions:

□ Enforce MFA for all users accessing critical maritime systems.

□ Implement biometric authentication for higher security levels, particularly for privileged accounts that can access ECDIS, telemetry systems, or loading programmes.

□ Use PKI Certificates or Secure Tokens for system-to-system authentication.

□ Use centralised security enforcing functions and data sources (i.e. a single Active Directory instance for user accounts and privileges).

□ Utilise the highest grade of encryption algorithm supported to protect the information in transit and at rest.

A2. Access Control Policies for Authorisation

Establish and enforce access control policies to ensure that only authorised users and systems can access critical data or infrastructure. These policies should support centralised management, simplifying control and enforcement across maritime operations. Security enforcing functions must not be distributed across the network, and is best practice to be centralised to ensure simplicity and consistency.

These policies can be enforced using centralised systems like Active Directory, which controls user access based on predefined rules. For instance, a crew member responsible for navigation should have access only to the systems necessary for their role, while administrative users would have different levels of access.

Implementation Actions:

□ Define access control policies for each role within the organisation.
□ Enforce a Role/Attribute Based Access Control based approach, as per NIS2.
□ Use centralised access management systems to enforce these policies.
□ Regularly review access permissions and adjust based on changes in roles or responsibilities.
□ Ensure that only authorised personnel have access to critical systems, applying the principle of least privilege.

A3. Password Management

Ensure that all systems and users adhere to strong password policies and regularly update their credentials to minimise the risk of password-related security breaches.

Password management involves setting policies that enforce password complexity (requiring a combination of upper/lowercase letters, numbers, and special characters) and regular password changes (every 90 days). PKI Certificates should be rotated annually or based on the risk exposure of the system.

For systems like navigation controls or telemetry communication terminals, password complexity helps prevent unauthorised access from brute-force attacks or phishing attempts.

It is best practice to store any user passwords in a secure and encrypted password vault, with MFA access enforced with proactive security monitoring on access.

Implementation Actions:

□ Set strong password policies for all users and systems, requiring a combination of letters, numbers, and symbols.
□ Enforce regular password changes (e.g., every 90 days) for all users.
□ Implement password expiration and reset policies for users and systems that have long periods of inactivity.

□ Ensure password vault tooling is available to securely store and manage passwords, reducing the risk of weak or reused passwords.

A4. Privileged Account Management

Closely monitor and manage privileged accounts, ensuring that they are granted only to users who need them, and that their activities are regularly audited to prevent misuse.

Privileged accounts have elevated access to critical systems and can make significant changes to configurations, so managing these accounts is critical for security. For example, administrative users who manage onboard systems or onshore networks should have their accounts closely monitored to protect against high-severity insider threats.

Additionally, privileged access should be regularly reviewed to ensure that only those who need it have it, and that unused privileges are revoked.

Implementation Actions:

□ Identify and catalogue all privileged accounts across the network.
□ Regularly review access rights to ensure they are still required.
□ Monitor privileged account activity for any suspicious actions or irregular activity.
□ Implement Just-In-Time (JIT) access for privileged users where possible, granting elevated privileges only when necessary and for limited periods.

A5. Access Based on Least Privilege

Ensure that access to systems and information is granted based on the principle of least privilege, meaning users and systems are only given the minimum permissions necessary to perform their tasks.

The principle of least privilege involves limiting access to only the resources and systems that are essential for a user or system to do their job - this helps minimise the risk of misuse or accidental damage.

For example, a crew member responsible for maintaining ship engines would only have access to engine-related systems, not navigation or communication systems. Similarly, administrative users would only have the necessary permissions to manage user accounts, but not critical ship controls.

Implementation Actions:

□ Conduct a review of all user and system roles to define necessary access.
□ Apply the least privilege principle when assigning access rights, limiting permissions to only what’s needed for each user role.

□ Regularly audit access rights to ensure no unnecessary privileges are granted.

□ Implement automated access reviews to ensure privileges are revoked when no longer needed (e.g., based on personnel joiner, mover, or leaver activity).

□ Protect access to USB ports and other removable device endpoints, based on job roles and operational requirements.

□ Enable device whitelisting, to restrict the usage of unauthorised or personal devices - allow only approved corporate devices that meet security standards, such as encryption and tamper-proof mechanisms.

□ Establish clear distinction of access rights between onboard and onshore personnel for maritime systems, following IMO guidelines.

A6. Account Provisioning and Deprovisioning

Ensure that accounts are provisioned and deprovisioned in a timely manner, reducing the risk of unused or orphaned accounts being exploited by attackers.

This process should be automated to ensure that access rights are adjusted immediately when personnel changes occur. For instance, when a crew member leaves the vessel, their access to onboard systems should be automatically revoked, or when staff leave the organisation.

Deprovisioning is critical to ensure that no inactive or unnecessary accounts remain on the network, as these could be targeted by malicious actors or former personnel for unauthorised access.

Implementation Actions:

□ Implement automated systems to manage account provisioning and deprovisioning based on employment status or role changes.

□ Regularly audit accounts to identify and disable any inactive or orphaned accounts.

□ Integrate account provisioning systems with human resources databases to trigger automatic updates for joiners, movers, and leavers.

A7. Access Reviews

Regularly review access rights across all systems to ensure that users have only the access necessary for their roles, and that any excessive privileges are identified and removed.

For example, during an access review, you might identify that a former crew or staff member still has access to critical communication systems, prompting immediate revocation.

Regular access reviews help identify discrepancies, unnecessary access, or misconfigurations that could pose security risks if not addressed.

Implementation Actions:

- □ Schedule regular access reviews (e.g., quarterly) across all critical systems.
- □ Use automated tools to generate reports that detail access permissions for each user, and their changes over time to mitigate against privilege growth.
- □ Work with department managers to validate that current access levels match user roles and responsibilities.
- □ Immediately remove or adjust access rights for users whose permissions exceed what is necessary for their role.

A8. Remote Access Security

Ensure that secure methods are used for remote access to critical maritime systems, especially when crews, engineers, privileged users or administrators need to access systems from external locations.

This is typically achieved using Virtual Private Networks (VPNs), Multi-Factor Authentication (MFA), MDM (Mobile Device Management), and strong encryption protocols to protect data in transit.

For example, when a ship's engineer needs to access the vessel's engine control system or telemetry communication system from shore, they should be required to use a VPN with MFA to ensure that the connection is secure and authenticated.

Implementation Actions:

- □ Configure the MDM solution to enforce robust security policies, such as mandatory device encryption, MFA, and automated device compliance checks.
- □ Implement VPNs with strong encryption for all remote connections to onboard systems (such as via SSH Port 22 or RDP Port 3389).
- □ Ensure that all remote sessions are logged and monitored for suspicious activity.
- □ Train crew members and administrators on best practices for secure remote access, including recognising phishing attempts or insecure networks.

Regulatory Compliance and Risk Management

Regulatory Compliance and Risk Management are essential components of maritime security governance, ensuring that organisations not only protect their operations from cyber threats but also adhere to the evolving regulatory landscape.

*This includes compliance with international frameworks such as **IMO MSC.428(98)** for maritime safety, the **NIS2 Directive** for protecting essential services within the EU, and **GDPR** for safeguarding personal data - by integrating compliance and risk management into daily operations, maritime organisations can enhance their security posture, protect critical systems, and avoid legislative action and significant financial penalties.*

R1. Risk Management

Ensure that cyber security risks are continuously identified, assessed, and managed throughout the lifecycle of systems, technologies, and operations. This risk-based approach allows maritime operators to proactively address potential threats before they can disrupt operations.

By continuously evaluating cyber security risks that the systems and network face, maritime companies can implement security controls to minimise vulnerabilities. For example, before deploying a new communication system onboard, a thorough risk assessment might identify the need for additional encryption or stronger access controls.

Implementation Actions:

□ Conduct regular threat modelling to identify potential attack vectors.

□ Use architecture reviews to assess how systems interact and where vulnerabilities might exist.

□ Perform technical security tests (e.g., penetration tests) to evaluate the resilience of critical systems.

□ Produce data protection impact assessments (DPIAs) to articulate the risks associated with processing PII, as per GDPR.

□ Continuously update risk management strategies as threats evolve.

□ Dedicate a Security Risk team to manage security risks through life, and define acceptable tolerance levels for severity and criticality.

R2. Regulatory Frameworks

Ensure compliance with all relevant cyber security regulations, standards, and frameworks such as NIS2, IMO MSC.428(98), NIST CSF, and GDPR.

Maritime operators must demonstrate documented compliance with global and regional regulations that govern cyber security. This includes adhering to the NIS2 EU Directive, IMO's cyber security guidelines, standards such as NIST CSF, and legislation such as GDPR. Regular audits and assessments are crucial to demonstrate that the company's systems and processes are aligned with these regulations, as they may be regularly required by auditors.

- **NIS2 Directive**
  The NIS2 Directive is the updated version of the NIS Directive, aimed at improving cyber security across the European Union. It applies to operators of essential services, including those in the maritime sector, and imposes stringent cyber security and reporting requirements and standards.
- **IMO MSC.428(98)**
  The IMO MSC guidelines provide a framework for managing maritime cyber security risks to ensure the safety of ships, cargo, and passengers. These guidelines were adopted in 2017 and require shipping companies to integrate cyber security risk management into their safety management systems (SMS) and closely aligns with NIST CSF.
- **NIST CSF 2.0**
  The National Institution of Standards and Technology Cyber Security Framework is a set of guidelines designed to help organisations manage and reduce cyber security risk. It consists of six core functions: Identify (understand risks and assets), Protect (safeguard systems), Detect (identify incidents), Respond (mitigate impacts), Recover (restore normal operations), and newly introduced Govern (assess compliance).
- **General Data Protection Regulation (GDPR)**
  While primarily focused on data security and privacy, GDPR has significant implications for cyber security, particularly for organisations that process PII (personally identifiable information) data. Maritime companies that handle data related to passengers, crew members, and contractors must comply with GDPR's stringent requirements for data protection and incident reporting, and are liable to significant penalties for non-compliance.

Implementation Actions:

□ Document compliance with relevant regulations – utilising evidence from a MARINE assessment will be able to provide a lot of the information required. A Mapping spreadsheet can be accompanied that displays the aligned security requirements between MARINE, NIS2, IMO, NIST CSF, and GDPR.

□ Review regulatory changes regularly to ensure ongoing compliance and understand updates.

□ Train personnel on regulatory requirements to ensure organisation-wide adherence.

□ Create a regulatory compliance checklist to audit compliance across the organisation.

□ Prepare for third-party auditors, as for example IMO compliance is enforced through audits and inspections.

R3. Compliance Audits

Conduct regular compliance audits to ensure that all systems, processes, and policies meet the required standards and regulations.

These audits can be conducted internally or by third-party auditors. For example, a compliance audit might assess whether onboard communication systems meet the cyber security requirements set forth as part of GDPR.

Implementation Actions:

□ Schedule periodic audits to assess cyber security compliance (at least every 6 months).
□ Document audit findings and take corrective actions to address any issues.
□ Use third-party auditors to ensure objectivity and a comprehensive review.
□ Track audit results over time to ensure continuous improvement in compliance.
□ Maintain an inventory (or record) of personal data processing activities, including details on what data is processed, the purpose, data retention periods, and who has access to it.

R4. Privacy Impact Assessments (PIAs)

Conduct Privacy Impact Assessments (PIAs) for any new systems or technologies to ensure compliance with data privacy regulations, as per GDPR.

Before introducing a new system that processes Personally Identifiable Information (PII, e.g., a crew management system or a passenger booking platform), a PIA should be conducted to evaluate how the system handles personal data and whether it complies with privacy laws. This assessment identifies privacy risks and helps implement appropriate security measures to protect personal data.

Implementation Actions:

□ Identify any new system or technology that processes PII data.
□ Conduct a PIA to assess privacy risks and determine compliance.
□ Implement measures to mitigate any identified risks, such as data encryption or access control.
□ Document the PIA results and update them regularly as the system evolves over time.

R5. Document Retention Policies

Establish document retention policies to ensure that all compliance-related documents are securely stored and retained for appropriate periods.

Document retention policies specify how long documents related to compliance (e.g., audit reports, risk assessments, PIAs) should be kept and where they should be stored. Secure repositories, either digital or physical, should be used to protect these documents from unauthorised access or destruction.

Implementation Actions:

□ Define document retention periods for compliance-related records (e.g., five years).
□ Use secure digital or physical storage solutions to safeguard documents.
□ Regularly audit document retention practices to ensure compliance.
□ Implement automated retention tools to manage document lifecycles.

R6. Data Protection Policies

Implement comprehensive data protection policies to ensure that personal and sensitive data is handled in compliance with privacy regulations, particularly GDPR.

These policies should include requirements for data encryption, access control, and secure deletion. For maritime operations, this could apply to systems managing passenger information, office staff, crew records, or vendor data.

Implementation Actions:

□ Ensure appropriate personnel have been assigned roles to support GDPR compliance, such as a DPO (Data Protection Officer) to monitor ongoing compliance, Data Controllers, and Data Processors.
□ Develop and implement data protection policies in line with NIS2 and GDPR requirements.
□ Ensure data is encrypted both at rest and in transit.
□ Protect PII data by ensuring data minimisation as a principle, obtaining consent for processing, and giving individuals rights to access and delete their data.
□ Restrict access to personal data to only those who need it for their roles.
□ Train personnel on data protection policies to ensure compliance organisation-wide.

R7. Data Breach Notification Procedures

When a data breach occurs, organisations must promptly notify affected individuals, regulators, and other relevant stakeholders, detailing the nature of the breach and the steps being taken to mitigate its impact.

For example, in the event of a security breach on an onboard system that exposes personnel or passenger data, the organisation should notify the relevant data protection authority (DPA) and take immediate actions to secure the affected systems.

Implementation Actions:

□ Establish data breach notification procedures, defining roles and timelines for communication.

□ Identify all relevant stakeholders who would need to be notified on occurrence of a breach, such as DPO and relevant customers or third-party organisations.

□ Ensure that procedures align with both relevant legislative requirements.

□ Train personnel to identify data breaches and initiate the notification process.

□ Regularly test and review the breach notification process to ensure readiness.

R8. Incident Reporting Requirements

Adhere to incident reporting requirements as specified by regulators such as NIS2. These requirements ensure that serious cyber security incidents are reported promptly and managed effectively.

When a cyber security incident occurs, organisations must report it to the relevant authorities within specified timeframes. This may include regulators, sectoral bodies, or incident response teams.

Implementation Actions:

□ Report incidents within 24 hours of identification, as per NIS2 (this is a faster timescale compared to GDPR, which states 72 hours).

□ Develop an incident reporting policy outlining when, how, and to which stakeholders' incidents must be reported to.

□ Establish clear communication lines with national cyber security authorities and maritime regulators.

□ Define and follow playbooks on recording all information and data related to the incident.

□ Train key personnel on incident reporting requirements and procedures.

□ Maintain a record of all incidents reported for audit and review purposes.

R9. Third-Party Management

Assess and manage cyber security risks associated with third-party vendors and service providers, ensuring that they meet your organisation's security standards and do not introduce vulnerabilities into your systems and network.

This includes conducting due diligence before engaging with a new vendor and requiring them to adhere to your cyber security policies. For example, a port service provider that connects to your vessel's systems must demonstrate compliance with your security requirements to prevent introducing vulnerabilities into your network.

Implementation Actions:

- □ Perform due diligence on all third-party vendors and suppliers before utilising their services.
- □ Include cyber security requirements in contracts with third parties, ensuring they comply with your organisation's security standards (such as MARINE).
- □ Regularly audit third-party security practices and monitor their access to your systems.
- □ Re-evaluate third-party relationships periodically to ensure ongoing security compliance (at least every 6 months).
- □ Request to have controlled visibility of any third-party supplier security scan or penetration test results for transparency.

R10. Continuous Monitoring for Compliance

Set up automated systems to continuously monitor compliance with cyber security frameworks, regulations, and risk management frameworks, enabling real-time updates and swift mitigation of any non-compliance issues.

Continuous monitoring systems provide real-time insights into an organisation's compliance status by tracking regulatory changes, system configurations, access controls, and data protection policies. These systems automatically detect deviations from established policies or regulatory requirements, allowing organisations to address non-compliance before it leads to a breach or penalty.

For example, continuous monitoring could flag a misconfiguration in the ship's telemetry communication system that fails to meet NIS2 encryption requirements, prompting immediate corrective action.

Implementation Actions:

- □ Ensure that the DPO is assigned the responsibilities and supporting Security & Compliance team to centrally monitor for compliance, as per GDPR.

□ Implement automated continuous monitoring tools that track compliance with NIS2, IMO MSC.428(98), and NIST CSF.

□ Set up automated alerts for any deviations from compliance standards.

□ Regularly review monitoring reports to ensure compliance status is up to date.

□ Enable a compliance roadmap to be established, to aim to improve the organisations security posture over time and improve compliance with the relevant standards.

Incident Response Planning

Incident Response Planning ensures that maritime organisations can quickly detect, mitigate, and recover from cybersecurity incidents. Through clear procedures, defined roles, and regular training, an effective response plan helps protect vessels and onshore operations from ever emerging cyber threats.

I1. Incident Response Plan

Develop and maintain a comprehensive Incident Response Plan (IRP) to ensure that your organisation can quickly detect, mitigate, and recover from cyber security incidents. A well-structured plan helps reduce downtime and the potential impact on critical maritime operations.

The plan should detail how incidents are detected, escalated, contained, and resolved. For example, if a ship's communication system is compromised, the IRP will define the steps to isolate the issue, notify stakeholders, and initiate recovery processes.

Implementation Actions:

□ Develop an IRP that covers detection, containment, eradication, and recovery from cyber incidents.

□ Outline Playbooks on differing types of potential compromise, such as malware propagation, ransomware, and insider threat.

□ Include details on who is responsible for handling specific types of incidents.

□ Ensure that the plan is accessible and regularly updated based on lessons learned from previous incidents.

□ Incorporate the IRP into the broader Safety Management System (SMS) and ISM (International Safety Management) Code.

I2. Incident Categorisation

Establish a clear categorisation scheme to categorise the criticality of incidents, to enable an appropriate and proportional response. Different types of incidents may require different responses based on their severity and potential impact.

Incidents should be categorised based on their severity and scope. For example, an incident affecting a single system might be categorised as low severity, whereas an attack impacting a deployed ship's navigation system would be high severity. Categorisation can include levels such as "low", "moderate", “high”, and "critical".

Implementation Actions:

□ Develop a categorisation system based on impact, severity, and criticality.
□ Train personnel to recognise different types of incidents and categorise them accurately.
□ Use categorisation as a basis for deciding escalation paths, resource allocation, and communication requirements.

I3. Response Team Roles

Clearly define the roles and responsibilities within the Incident Response Team (IRT) to ensure a coordinated and efficient response to incidents.

Each member of the Incident Response Team should have clearly defined roles, such as Incident Commander, Communications Manager, and Technical Lead. The Incident Commander oversees the entire response process, while the Technical Lead focuses on addressing the technical aspects of the incident.

Implementation Actions:

□ Define roles within the IRT, such as:
  ○ Incident Commander, Communication Manager, and Technical Lead.
□ Create a clear escalation chain and communication protocol for the response team.
□ Ensure that roles are assigned to specific individuals and that backups are in place.
□ Ensure that all personnel within the roles are sufficiently trained and regularly practice the IRP and associated Playbooks.

I4. Communication Plan

Create a Communication Plan to ensure timely and effective communication during a cyber security incident, both internally and externally.

The communication plan should define how information is shared during a cyber incident. This includes notifying stakeholders such as the crew, onshore teams, regulators, customers, and third parties. The plan should also address how to communicate with external parties like cyber security authorities or data protection bodies, especially in the case of incidents affecting sensitive data to comply with legislation.

Implementation Actions:

□ Establish a communication protocol for notifying internal and external stakeholders, as per the IMO SMS (Safety Management System).

□ Designate specific individuals to handle internal and external communication during an incident as part of the Response Team Roles.

□ Include predefined templates for incident notifications for consistency and speed during an incident.

□ Define clear commination channels and personnel for authoritative points of contact, such as National CSIRT (Cyber Security Incident Response Teams) teams.

□ Incidents must be reported within 24 hours of identification, as per NIS2.

I5. Intrusion Detection Response

Automated detection tools such as Intrusion Detection Systems (IDS) continuously monitor networks and systems for abnormal activities. These tools generate alerts when suspicious activities, such as unauthorised access or malware, are detected. In maritime operations, these tools are particularly useful for monitoring onboard systems, which may be remotely accessed or controlled by onshore systems, and therefore potentially targeted by adversaries.

Implementation Actions:

□ Deploy automated detection tools across both onboard and onshore systems.

□ Integrate tools with a centralised incident response system and centralised logging systems (i.e. the SIEM) to enable real-time monitoring.

□ Integrate tools with a corresponding Intrusion Prevention System (IPS) for consistency and shared analytics.

□ Regularly update detection tools to ensure they recognise the latest threats and vulnerabilities.

I6. Incident Response Training

Provide regular incident response training to personnel, ensuring they are prepared to respond to cyber security incidents in a timely and effective manner.

Incident response training includes tabletop exercises, simulations, and drills that replicate real-world scenarios. These exercises help identify gaps in the IRP and provide practical experience for personnel in dealing with cyber incidents. For example, a tabletop exercise might simulate a ransomware attack on the ship's communication systems, allowing the response team to practice their procedures and enact any applicable Playbooks based on the simulated incident's criticality categorisation.

Implementation Actions:

- □ Conduct regular tabletop exercises and simulated cyber incident drills.
- □ Evaluate the effectiveness of training exercises and refine the IRP based on lessons learned.
- □ Train both onboard crew and onshore teams on how to handle different types of incidents.
- □ Encourage a blame-free culture during exercises to ensure a safe and open training environment.

I7. Backup, Resilience, and Disaster Recovery

Define and regularly test backup, resilience, and Disaster Recovery (DR) procedures to ensure that critical data and systems can be protected during and after cyber security incidents.

Backup and recovery are critical components within incident response and business continuity planning (BCP) processes. Organisations must have systems in place to back up critical data, such as navigation charts, ship logs, ECDIS configuration, cargo loading plans, and crew information.

Regular testing of these systems ensures that data can be restored quickly in the event of an attack, such as a ransomware incident, where access to critical files might be restricted indefinitely.

Implementation Actions:

- □ Implement automated backup systems for onboard and onshore data.
- □ Incorporate immutable backup solutions to protect data integrity and prevent unauthorised modifications, including physical backups such as on dedicated tamper-proof hard drives.
- □ Implement a physical backup cadence for more sensitive systems at a regular period, which are isolated and separate to digital automated backups.
- □ Ensure critical backup systems and information is isolated from the primary network.
- □ Establish failover systems and redundant infrastructure to sustain operations.
- □ Develop and maintain a disaster recovery (DR) plan that integrates backup and recovery processes alongside broader strategies for restoring operations.

I8. Post-Incident Review

Conduct a Post-Incident Review to analyse how the incident was handled, and identify areas for improvement in the incident response process.

After an incident has been resolved, a post-incident review involves gathering the incident response team to discuss what went well, what didn't, and how future responses can be improved. This review helps refine the Incident Response Plan (IRP) and ensures that any lessons learned are applied.

For example, if a phishing attack led to unauthorised access to onboard systems, the review might lead to additional training for crew members and onshore staff.

Implementation Actions:

- □ Conduct a post-incident review after each incident, involving all relevant stakeholders.
- □ Document lessons learned and incorporate them into the revised IRP.

I9. Forensic Analysis

Establish protocols for conducting Forensic Analysis following a cyber security incident to determine how the breach occurred, and what data or systems were impacted.

Forensic analysis involves gathering evidence, such as system logs and network traffic data, to identify the root cause of an incident. This process can help determine how an attacker gained access to the system and what actions they took. In a maritime setting, forensic analysis might be used to trace how malware entered the ships infrastructure, and if it impacted any onboard or onshore systems.

Implementation Actions:

- □ Establish forensic analysis procedures to follow after an incident has been contained.
- □ Train dedicated personnel in forensic data collection and integrity, ensuring evidence is preserved for investigation and stored securely in an environment disconnected from the primary network.
- □ Analyse the collected data methodically, looking for indicators of compromise (IoCs), malicious activity, and patterns. All findings must be documented, including timestamps, methods, and tools used, to provide a clear trail of the investigation.
- □ Use forensic findings to inform incident response improvements and prevent recurrence.

I10. Testing Incident Response Plans

Regularly test and update your Incident Response Plan (IRP) to ensure it remains effective in addressing current and emerging threats.

Testing the IRP involves conducting drills, simulations, and audits to verify that the plan works as expected. This includes simulating cyberattacks, such as ransomware incidents or DDoS attacks, to test how quickly the organisation can detect, mitigate, and recover from an incident. Regular updates to the IRP ensure that it remains aligned with evolving cyber security threats and technologies.

Implementation Actions:

□ Schedule regular IRP tests, including both tabletop exercises and live simulations.

□ Ensure all relevant personnel are involved in testing, from onboard crew to onshore IT personnel.

□ Update the IRP based on test outcomes and lessons learned.

Network Security

Network security is crucial in maritime operations as it protects the integrity, confidentiality, and availability of onboard and onshore systems ability to communicate and process information. With the increasing digitalisation of vessels, navigation, cargo management, and onshore infrastructure being connected via networks, this makes them vulnerable to cyber threats and therefore requires appropriate protective security controls.

Robust network security measures, including firewalls, intrusion prevention systems, strong encryption, and proactive monitoring, are vital to preventing unauthorised access and network based attacks.

N1. Firewalls

Firewalls are critical in protecting network boundaries by filtering ingress and egress network traffic based on predefined security rules. They act as a first line of defence, preventing unauthorised access to systems and the network. Securely configured firewalls can significantly reduce the risk of external threats and ensure only legitimate traffic flows through the network.

Implementation Actions:

□ Define security policies and rules to allow only necessary traffic.

□ Implement a “whitelist" approach for only allowing specified incoming protocols and IP addresses.

□ Regularly update firewall rules to address new threats – ensure an appropriate review and change process is enforced when modifying the network firewalls rules.

□ Integrate firewalls with SIEM (Security Information and Event Management) systems for comprehensive security monitoring of network logs.

□ Regularly test the Firewall for its capacity to allow authorised traffic, block anything that is not specified via the security policies, and withstands network-based attacks such as DDoS.

N2. Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems (IPS) monitor network traffic for signs of malicious activity, such as malware or abnormal behaviour, and automatically take actions to block or mitigate these threats. They complement firewalls by providing deeper inspection of network packets and can help detect more sophisticated attacks that bypass basic firewall controls.

Implementation Actions:

□ Deploy IPS devices at critical points within the network, such as ingress points and internal segments.

□ Configure IPS rules to detect known threats and suspicious patterns that are automatically updated based on threat signatures.

□ Customise rules based on the specific network environment and required communication channels.

□ Test IPS configurations to ensure they do not block legitimate traffic.

□ Monitor and review IPS alerts to refine detection capabilities.

N3. Network Segmentation

Network segmentation involves dividing a network into smaller, isolated segments to limit access and contain potential security breaches. By segmenting networks, organisations can protect critical systems and data from unauthorised access and prevent attackers from easily traversing across the network. Without segmentation, attackers can have unilateral freedom to compromise systems within the network, including any dependant services within third-party networks.

Implementation Actions:

□ Identify and categorise network assets to determine which systems need to be segmented.

□ Map out network architecture to identify critical infrastructure components.

□ Divide the network into distinct zones (such as internal network, DMZ, customer public network, management network) based on function, sensitivity, and security requirements.

□ Use VLANs or Subnets to create separate network segments. VLANs allow you to group infrastructure by function or security level, even if they are physically located on different network switches, facilitating better traffic management.

□ Isolate user-facing systems from sensitive, non-user-facing systems.

□ Regularly test segmentation controls to ensure they are properly implemented.

□ Comply with NIS2 requirements for protecting critical infrastructure networks.

N4. Secure Configuration

Secure configuration involves hardening network devices and systems to minimise vulnerabilities and enforce least privilege. This includes disabling unnecessary services, enforcing strong password policies, regularly updating configurations, and enforcing a frequent patching cadence. Securely configured devices reduce the attack surface and help protect against unauthorised access or network exploitation.

Implementation Actions:

□ Develop and enforce configuration baselines for all network devices.
□ Disable unused services and ports to limit potential attack vectors – a particular focus on management ports must be restricted (such as port 22 (SSH) and 3389 (RDP)).
□ Regularly review and update configurations in line with best practices.
□ Implement strong password policies and enforce multi-factor authentication.
□ Maintain a detailed inventory of device configurations and changes.
□ Conduct regular security testing to verify compliance with configuration standards.

N5. Encryption of Data in Transit

Encryption of data in transit ensures that sensitive information remains secure while being transferred across networks. By encrypting data, organisations can protect against interception and unauthorised access during transmission, ensuring information integrity and confidentiality. This is essential for safeguarding confidential communications and complying with regulations such as NIS2.

Implementation Actions:

□ Use secure protocols (e.g., TLS, IPsec) to encrypt data during transmission.
□ Ensure cryptographic keys are managed securely and periodically rotated.
□ Configure network devices to enforce encryption for all sensitive data transfers.
□ Use end-to-end encryption for communications between systems and applications.
□ Test encryption setups to confirm that data remains secure throughout the transmission.
□ Monitor for any unauthorised attempts to access or intercept encrypted data.
□ Never use any custom encryption protocols – only recognised next-generation approved algorithms.

N6. Encryption of Data at Rest

Encrypting data at rest ensures that sensitive information stored on devices, servers, and databases is protected from unauthorised access and compromise. Even if physical devices are compromised, encryption helps maintain the confidentiality of the data, making it unreadable without the correct decryption key.

Implementation Actions:

□ Implement encryption for all sensitive data stored on servers, databases, and storage devices.
□ Use strong, industry-approved encryption algorithms (e.g., AES-256).
□ Securely manage and store encryption keys, following best practices for key management.
□ Regularly audit encrypted data to verify compliance with encryption policies.
□ Integrate encryption with access controls to ensure only authorised users can decrypt the data.
□ Ensure secure installation and regular auditing of Hardware Security Modules (HSMs), with strict access controls and monitored physical security to protect the most sensitive encryption keys.
□ Comply with industry standards, such as IMO MSC.428(98), for maritime systems.

N7. Virtual Private Networks (VPN)

VPNs provide secure remote access to a network by encrypting traffic between the user's device and the network. This ensures that data sent and received remains confidential, protecting against interception, particularly when accessing the network from public or third-party networks.

Implementation Actions:

□ Deploy VPN solutions that use strong encryption protocols (e.g., IPsec, OpenVPN).
□ Generate and install server and client certificates via an authorised Certificate Authority (CA) to enable encrypted, authenticated connections for the VPN.
□ Configure VPNs to enforce MFA for user access.
□ Limit VPN access to only necessary users and services, following the principle of least privilege.
□ Monitor VPN usage and establish alerts for unusual login patterns or access attempts.
□ Regularly update VPN software to address any vulnerabilities.
□ Ensure VPN connections terminate and re-authenticate after a set period to reduce security risks (recommended every 8-24 hours).

N8. Penetration Testing

Penetration testing involves simulating security attacks on a network to identify vulnerabilities and weaknesses. By performing regular security tests, organisations can proactively discover and address security gaps, ensuring better protection against potential threats and enforcing a robust cyber defence.

Implementation Actions:

□ Schedule regular penetration tests (e.g., every 6 months) with certified security vendors to evaluate network security controls.
□ Focus on critical systems and high-risk network areas to prioritise testing efforts.
□ As a priority review test output reports, and implement remediation activities to address any identified vulnerabilities.
□ Retest after remediation to verify that security issues have been resolved.

N9. Patch Management

Patch management ensures that all network devices, software, and systems are regularly updated to address known vulnerabilities within the CVE database. Applying patches promptly and at a regular cadence reduces the risk of exploitation.

Implementation Actions:

□ Maintain an inventory of all network devices and systems to track any required updates.
□ Document and track the patch management process, including applied updates and changes.
□ Set up a regular schedule for applying patches and updates, prioritising critical fixes.
□ Test patches in a controlled environment before deploying them to live systems for effective change management.
□ Enable automatic updates where possible, particularly for security-critical components (and only enforce the changes after automated regression testing).
□ Monitor for newly discovered vulnerabilities and apply out-of-band patches as needed based on subscription to threat intelligence feeds.

N10. Data Localisation and Network Boundaries

Data localisation and network boundaries ensure compliance with regulations regarding the storage and transfer of data. NIS2 specifically requires that data, especially sensitive information, remains within controlled environments and that measures are in place to protect data crossing EU borders.

Implementation Actions:

□ Identify and categorise data to determine localisation and legislative processing requirements.
□ Configure network boundaries to manage data flow between internal and external networks.
□ Implement geofencing to restrict data movement to specific regions or networks (for example, specifying only the approved Regions if using AWS Cloud).

□ Regularly audit data storage locations to ensure compliance with regulatory requirements.
□ Monitor data traffic crossing network boundaries and detect any unauthorised transfers.

Education

Education in cyber security is essential to ensure that crew members, shore-based personnel, and stakeholders understand and are aware of the risks and security best practices associated with systems and networks on vessels and onshore. As ships become more connected, human error can be a significant factor in security incidents. Regular training and awareness programs build a security-conscious culture, reducing the likelihood of misconfigurations.

A well-educated workforce can respond more effectively to potential threats and incidents, ensuring swift and appropriate actions to mitigate risks. By providing ongoing education on the latest security trends, regulations, and technologies, fostering a more robust and resilient cyber security posture and growing the security capabilities of the workforce.

E1. Security Awareness Training

Ongoing security awareness training helps all employees understand cyber security risks, policies, and best practices. This ensures that personnel are aware of potential threats and know how to recognise and avoid them. Training should be regularly updated to address new threats and comply with standards like NIS2.

Implementation Actions:

□ Develop a mandatory training program covering essential security principles, company policies, and data processing security.

□ Schedule regular refresher courses to reinforce key topics.

□ Monitor participation and track knowledge retention over time.

□ Allow personnel to request attendance at external training courses, especially in emerging technologies such as Artificial Intelligence (AI), Cloud, and Quantum Computing.

E2. Phishing Simulations

Phishing simulations are designed to test how employees respond to phishing attempts, helping to identify vulnerabilities and improve security awareness. By simulating real-world scenarios, organisations can educate personnel on how to recognise and report suspicious emails, reducing the risk of successful attacks, and how personnel can report them appropriately.

Implementation Actions:

□ Design realistic phishing scenarios and conduct regular simulations.

□ Provide immediate feedback and training to those who respond incorrectly, whilst fostering a blame-free culture and encourage education.
□ Use the results to identify trends and improve overall awareness, with suggested training courses provided.

E3. Incident Response Drills

Incident response drills help test the readiness of teams to respond effectively to cyber security incidents. Regular drills allow organisations to evaluate their incident response plans, identify weaknesses, and ensure that personnel are well-prepared to handle real-world scenarios.

Implementation Actions:

□ Conduct drills regularly involving key personnel across all IT departments.
□ Evaluate responses and identify areas for improvement.
□ Update the incident response plan based on lessons learned from each drill.
□ Ensure coordination between onboard and onshore teams for real time simulations for maritime operations.

E4. Role-Specific Training

Role-specific training focuses on providing tailored cyber security education to individuals in sensitive positions, such as privileged users and administrators. This ensures that those with access to critical systems understand the specific security protocols and responsibilities associated with their roles, and the best practices around operating in them.

Implementation Actions:

□ Develop content specific to roles that handle sensitive systems or data.
□ Include modules on secure configurations, access controls, and incident response.
□ Require assessments to verify understanding and readiness.
□ Raise awareness on the security controls enforced to manage privileged user and administrator roles, i.e. the auditing and monitoring controls that will record their actions for malpractice.

E5. Continuous Learning Opportunities

Encouraging continuous learning in cyber security helps personnel stay informed about the latest developments and threats. This can be achieved through ongoing education, workshops, webinars, and professional development programs. Continuous learning fosters a proactive security culture, essential in a constantly evolving threat landscape and upskilling staff.

Implementation Actions:

- □ Provide access to external courses, webinars, and professional development opportunities.
- □ Host internal seminars to discuss emerging threats and industry updates.
- □ Recognise and incentivise personnel who pursue further cyber security education.
- □ Encourage personnel to achieve industry recognised cyber security certifications, such as CISSP or OSCP.
- □ Foster a culture of security and data protection by promoting awareness campaigns and providing accessible resources related to both cyber security and data protection.

Assessment Scoring

A tiered scoring system is utilised to determine the level and strength of compliance against each specified Security Control. This score will be applied to every Security Control from each of the six core Categories within MARINE, with the average being taken to assign an overall score for each Category.

Score	Tier	Description
0	**Not Implemented**	The Control or requirement has not been implemented at all - no evidence or processes are in place to demonstrate compliance.
1	**Introductory Compliance**	The Control is implemented to a very basic level - there may be some introductory processes or technical controls in place, but they lack formalisation or documentation.
2	**Intermediate Compliance**	The Control is implemented with some degree of effectiveness. Basic documentation exists, personnel have received minimal training, and technical controls have been configured, but there may still be gaps in execution or oversight.
3	**Advanced Compliance**	The Control is fully implemented and operating as intended. Comprehensive documentation is available, regular training is conducted, ongoing monitoring processes are in place, and technical controls have been implemented and robustly tested to ensure compliance and effectiveness.

- End of Document -