Certificate in Maritime Data Analytics

Maritime Cybersecurity and Data Privacy

Cybersecurity in the maritime domain refers to the protection of vessels, ports, offshore installations, and related information systems from unauthorized access, disruption, or damage. The maritime environment is unique because it combines traditional navigation and cargo operations with modern digital technologies such as satellite communications, automated identification systems, and integrated bridge and engine controls. Understanding the specific terminology that underpins maritime cyber risk management is essential for anyone studying the Certificate in Maritime Data Analytics. The following explanation covers the most important terms and concepts, providing definitions, practical examples, and discussion of the challenges that professionals may encounter.

Asset describes any element that has value to a maritime operation. Assets can be physical, such as a ship's propulsion system, a port's crane, or a navigation buoy. They can also be digital, including the software that runs a vessel's dynamic positioning system, the databases that store cargo manifests, or the communication links that enable shore-to-ship coordination. Recognising what constitutes an asset is the first step in any risk assessment because the protection measures applied must be proportionate to the value and criticality of the asset.

Threat is any circumstance or event with the potential to cause harm to an asset. In maritime cyber contexts, threats range from deliberate attacks by nation-state actors, organized crime groups, or hacktivists, to accidental incidents such as mis-configuration of network devices, insider mistakes, or software bugs. For example, a ransomware campaign that targets ship-to-shore data exchange portals represents a threat that could delay cargo off-loading, cause financial loss, and disrupt supply chains.

Vulnerability is a weakness in a system, process, or control that can be exploited by a threat. Vulnerabilities may arise from outdated software, insecure default passwords, lack of encryption, or insufficient segmentation between operational technology (OT) and information technology (IT) networks. A common maritime vulnerability is the use of legacy navigation equipment that runs on unsupported operating systems, making it difficult to apply security patches.

Risk is the combination of the likelihood that a threat will exploit a vulnerability and the impact that such exploitation would have on the organization. Risk is often expressed as a function of probability and consequence. In the maritime sector, risk calculations must consider both safety implications (e.g., a compromised steering system leading to a collision) and business impacts (e.g., loss of revenue due to delayed shipments).

Incident refers to any event that compromises the confidentiality, integrity, or availability of a maritime information system. Incidents can be benign, such as a failed login attempt, or severe, such as a successful

intrusion that manipulates a vessel's ballast control system. An incident response plan typically includes detection, containment, eradication, recovery, and post-incident analysis.

Malware is malicious software designed to infiltrate, damage, or disrupt computer systems. Types of malware relevant to maritime environments include viruses, worms, Trojans, and spyware. A notable example is a Trojan that masquerades as a legitimate ship-performance monitoring tool but secretly exfiltrates navigation data to an external server.

Ransomware is a subset of malware that encrypts data and demands payment for the decryption key. The maritime sector has seen several high-profile ransomware attacks where ship operators were forced to pay to regain access to critical operational data. Because many maritime systems are time-sensitive, the impact of ransomware can be magnified when a vessel's voyage plan is locked during a narrow weather window.

Phishing is a social-engineering technique that attempts to trick users into revealing credentials or downloading malicious content. In a maritime setting, phishing emails may appear to come from a ship's charterer, a port authority, or a logistics partner, prompting the recipient to click a link that installs a backdoor on the ship's internal network.

Advanced Persistent Threat (APT) denotes a sophisticated, long-term attack campaign typically carried out by well-funded actors such as nation-states. APTs often target high-value maritime assets like strategic shipping lanes, oil tankers, or naval vessels. The goal may be espionage, sabotage, or the collection of sensitive cargo information. An APT may use multiple stages, including initial compromise via spear-phishing, lateral movement across networks, and data exfiltration through encrypted channels.

Internet of Things (IoT) refers to interconnected devices that collect and exchange data. Maritime IoT devices include sensor-enabled containers, smart buoys, and wearables for crew health monitoring. While IoT brings operational efficiency, each device can become an entry point for attackers if not properly secured. For instance, a temperature sensor on a refrigerated container that communicates over an unsecured Wi-Fi network could be hijacked to send false temperature readings, jeopardising cargo integrity.

Operational Technology (OT) encompasses the hardware and software that directly monitors or controls physical devices, processes, and events in the maritime environment. OT includes navigation systems, engine control units, automated cargo handling equipment, and safety monitoring devices. OT systems often have real-time constraints and may run on proprietary protocols, making them distinct from traditional IT systems.

Supervisory Control and Data Acquisition (SCADA) is a subset of OT used to gather and analyse real-time data from sensors and to issue control commands to equipment. In a port terminal, SCADA may manage crane operations, gate access, and power distribution. SCADA networks are attractive targets because compromising them can disrupt cargo flow or cause physical damage.

Automatic Identification System (AIS) is a maritime communication technology that automatically

broadcasts a vessel's identity, position, speed, and course. AIS data is used for collision avoidance, traffic monitoring, and situational awareness. However, AIS can be spoofed, meaning an attacker transmits false AIS messages to mislead other vessels or shore-based monitoring systems. An example of AIS spoofing is the creation of phantom vessels on maritime traffic maps, potentially causing unnecessary evasive actions.

Global Positioning System (GPS) Spoofing involves transmitting counterfeit GPS signals to deceive a receiver's location calculation. A ship's navigation system that relies on GPS could be led off course, potentially into hazardous waters. Spoofing attacks can be subtle, with the attacker gradually shifting position data to avoid detection.

Satellite Communication (SATCOM) provides voice and data connectivity for vessels at sea. SATCOM links are essential for transmitting weather updates, crew welfare communications, and operational data to shore. Because SATCOM relies on radio frequencies, it is vulnerable to interception, jamming, and unauthorized access if encryption is not applied.

Very High Frequency (VHF) Radio is the primary voice communication method for ship-to-ship and ship-to-shore interactions. While VHF is traditionally considered a low-risk medium, modern digital VHF radios can carry data services, and unencrypted transmissions can be intercepted by adversaries with suitable equipment.

Network Segmentation is the practice of dividing a larger network into smaller, isolated subnetworks to limit the spread of malware and restrict access to critical systems. In a maritime context, segmentation typically separates the bridge network (used for navigation) from the engine room network (used for propulsion control) and from the crew welfare network (used for internet access). Proper segmentation reduces the attack surface and contains breaches.

Firewalls are devices or software that enforce security policies by controlling inbound and outbound traffic based on predefined rules. A maritime firewall may block external connections to the vessel's navigation system while allowing secure, authenticated connections from shore-based monitoring platforms. Deploying firewalls on both the ship and at port facilities is a common defensive measure.

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are technologies that monitor network traffic for signs of malicious activity. An IDS alerts administrators when suspicious patterns are detected, while an IPS can automatically block the offending traffic. In maritime environments, an IDS may be configured to detect unusual command sequences sent to a vessel's engine control system, indicating a possible intrusion attempt.

Encryption is the process of converting data into a coded format that can only be read by parties possessing the appropriate decryption key. Encryption protects data in transit (e.g., over SATCOM links) and at rest (e.g., stored on shipboard servers). Strong encryption algorithms such as AES-256 are recommended for maritime data that includes cargo manifests, crew personal information, and navigation routes.

Virtual Private Network (VPN) creates a secure tunnel between a remote user and a private network, ensuring that data transmitted over public networks remains confidential and tamper-proof. Crew members accessing shipboard systems from shore, or port operators accessing terminal management platforms, often use VPNs to protect credentials and operational data.

Authentication verifies the identity of a user, device, or system before granting access to resources. Maritime authentication mechanisms range from simple passwords to more robust solutions such as digital certificates and biometric verification. Multi-factor authentication (MFA) combines two or more methods—something the user knows (a password), something the user has (a token), and something the user is (a fingerprint)—to enhance security.

Access Control defines who is permitted to view or modify resources. Access control models commonly used in maritime IT include Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). For example, an engineer may have read-only access to the vessel's engine performance logs, while a captain may have full control over navigation settings.

Least Privilege is the principle that users and processes should be granted only the permissions necessary to perform their functions. Applying least privilege reduces the risk that a compromised account can be used to access critical systems. In practice, a ship's crew member might be allowed to view the weather forecast but not to alter the autopilot parameters.

Patch Management involves the systematic identification, testing, and deployment of software updates to fix security flaws. Maritime IT environments often depend on vendor-specific equipment with proprietary firmware, making patch management challenging. Delays in applying patches can leave vessels exposed to known exploits, especially when operating in remote regions with limited connectivity.

Incident Response is the coordinated approach taken to manage and mitigate the effects of a security incident. An incident response plan typically outlines roles and responsibilities, communication protocols, and step-by-step procedures for containment, eradication, and recovery. Effective incident response in maritime settings must consider the unique constraints of vessels at sea, such as limited bandwidth and the need for crew safety.

Cyber Resilience goes beyond prevention to encompass the ability of an organization to continue operating during and after a cyber event. Resilience strategies include redundancy in communication links, backup navigation systems, and regular drills that simulate cyber-attack scenarios. A resilient maritime operation can maintain essential functions such as safe navigation and cargo handling even when parts of its digital infrastructure are compromised.

Cyber Hygiene denotes the routine practices that help maintain a secure environment. Examples include regular password changes, disabling unused services, conducting vulnerability scans, and educating crew members about phishing tactics. Good cyber hygiene is a cost-effective way to reduce the likelihood of successful attacks.

Data Privacy concerns the protection of personal and sensitive information from unauthorized disclosure. In the maritime sector, data privacy issues arise with crew personal data, passenger records, cargo details, and contractual information. Compliance with privacy regulations such as the General Data Protection Regulation (GDPR) and the United Nations Convention on the Law of the Sea (UNCLOS) is increasingly important for global operators.

Personal Data is any information relating to an identified or identifiable individual. For a shipping company, personal data may include crew passports, medical records, and contact details. Protecting personal data requires both technical safeguards (encryption, access controls) and organizational measures (privacy policies, data-handling procedures).

GDPR is a comprehensive European data protection regulation that imposes strict obligations on organisations that process personal data of EU citizens. Although GDPR is European, its extraterritorial reach means that any maritime operator handling EU crew data must comply. Key GDPR concepts relevant to maritime include the rights to data access, rectification, erasure, and the requirement to report breaches within 72 hours.

IMO Guidelines refer to the International Maritime Organization's set of recommendations and standards for maritime cyber risk management. Notable documents include IMO Resolution A.1062, which calls for the adoption of a cyber risk management framework, and IMO Circular MSC.428(98), which provides practical guidance on protecting shipboard information systems. These guidelines encourage the integration of cyber considerations into existing safety management systems (SMS).

Safety Management System (SMS) is a structured approach used by ship owners and operators to ensure safe operation and compliance with regulations. The SMS now often incorporates cyber risk management as a component, recognising that cyber incidents can have safety implications. For example, a compromised alarm system could lead to delayed emergency response.

Risk Assessment is the systematic process of identifying, analysing, and evaluating risks. In maritime cyber contexts, risk assessments typically involve mapping assets, identifying threats and vulnerabilities, estimating likelihood, and determining potential impacts. The outcome guides the selection of appropriate controls and informs resource allocation.

Control denotes any safeguard or countermeasure implemented to reduce risk. Controls can be technical (e.g., firewalls, encryption), procedural (e.g., incident response playbooks), or physical (e.g., locked server rooms). Selecting effective controls requires balancing security, operational efficiency, and cost.

Security Policy is a formal document that outlines an organisation's security objectives, responsibilities, and rules. A maritime security policy may address topics such as acceptable use of shipboard computers, remote access procedures, and incident reporting requirements. Policies provide the foundation for consistent security practices across vessels and shore facilities.

Threat Intelligence is the collection and analysis of information about existing or emerging threats. Maritime organisations may subscribe to threat intelligence feeds that report on new ransomware variants, known APT groups targeting the shipping industry, or vulnerabilities in maritime navigation software. Integrating threat intelligence into security operations enables proactive defence.

Vulnerability Scan is an automated process that examines systems for known weaknesses. Scanning tools can discover missing patches, default credentials, and misconfigured services on shipboard servers. Regular vulnerability scans are essential because maritime networks often contain a mix of legacy and modern equipment.

Penetration Testing (or "pen-test") involves simulated attacks performed by authorised security professionals to evaluate the effectiveness of controls. In a maritime pen-test, testers might attempt to gain unauthorised access to a vessel's bridge network, bypass firewalls, or exfiltrate cargo data. Results help organisations understand real-world exploitability and prioritise remediation.

Supply Chain Security focuses on protecting the hardware and software components that flow into the maritime ecosystem. Threats such as counterfeit navigation equipment, malicious firmware updates, or compromised third-party logistics platforms can introduce vulnerabilities. Ensuring provenance of components and verifying the integrity of software updates are critical supply-chain security practices.

Zero-Trust Architecture is a security model that assumes no implicit trust, even within the internal network. Access is granted based on continuous verification of identity, device health, and context. Implementing zero-trust on a vessel may involve micro-segmentation of the bridge network, strict authentication for every command, and real-time monitoring of device behaviour.

Digital Twin refers to a virtual replica of a physical asset, such as a ship's propulsion system or a port's container yard. Digital twins are used for simulation, performance optimisation, and predictive maintenance. However, because they rely on data exchange between the physical and virtual worlds, they also become a new attack surface. Securing the data pipelines that feed the digital twin is therefore a priority.

Machine Learning (ML) and Artificial Intelligence (AI) are increasingly applied to maritime data analytics for tasks such as anomaly detection, route optimisation, and fuel consumption forecasting. While ML can enhance operational efficiency, the models themselves may be vulnerable to adversarial attacks that manipulate input data to cause incorrect predictions. Understanding the security implications of AI in maritime contexts is an emerging area of focus.

Anomaly Detection is the process of identifying data points that deviate from established patterns. In a ship's network, anomaly detection systems might flag abnormal traffic volumes, unexpected command sequences, or irregular sensor readings. Effective anomaly detection requires baseline data, continuous learning, and the ability to distinguish between benign variations (e.g., weather-related changes) and malicious activity.

Data Governance encompasses the policies, procedures, and standards that ensure data quality, security, and compliance. Maritime data governance programs define who can collect, store, process, and share data such as cargo manifests, crew schedules, and fuel consumption logs. Strong governance helps prevent data leakage and supports regulatory compliance.

Data Classification is the practice of categorising data based on sensitivity and required protection levels. For example, a ship's navigation charts may be classified as "confidential," crew medical records as "restricted," and publicly available AIS data as "public." Classification informs the selection of encryption, access controls, and handling procedures.

Data Minimisation is a privacy principle that recommends collecting only the data necessary to achieve a specific purpose. In maritime operations, this might mean storing only the essential crew identifiers for payroll, rather than retaining full biometric data once the payroll process is complete. Minimising data reduces the impact of a potential breach.

Data Retention defines how long data is kept before it is securely destroyed. Regulations often prescribe retention periods for specific types of data; for instance, crew employment records may need to be retained for a set number of years. Implementing automated retention schedules helps avoid unnecessary storage of outdated information.

Data Breach occurs when confidential, integral, or available data is accessed or disclosed without authorisation. A breach in the maritime sector could involve the theft of cargo manifest details, exposing a vessel's cargo to criminal exploitation, or the exposure of crew personal details, leading to identity theft. Prompt detection and reporting are essential to mitigate damage.

Data Exfiltration is the unauthorised transfer of data from a system to an external destination. Attackers may use covert channels, encrypted tunnels, or compromised satellite links to exfiltrate sensitive maritime data. Detecting exfiltration often requires monitoring outbound traffic for anomalies, such as unusually large data transfers during off-peak hours.

Secure Coding refers to the practice of developing software that is resilient to common vulnerabilities. Maritime software developers should follow standards such as OWASP Top Ten and apply techniques like input validation, proper error handling, and avoidance of hard-coded credentials. Secure coding reduces the risk that an application becomes an entry point for attackers.

Patch Tuesday is an informal term for the day each month when many software vendors release security updates. Maritime organisations must align patch deployment schedules with operational constraints, ensuring that critical shipboard systems are updated without disrupting voyages. In some cases, a "maintenance window" is defined to apply patches during port calls.

Remote Access enables users to connect to shipboard systems from a distant location. While remote access is indispensable for technical support and crew welfare, it also introduces security challenges. Secure remote

access solutions employ VPNs, strong authentication, and strict session monitoring to prevent unauthorised entry.

Red Team exercises simulate real-world attacks to test an organisation's defensive capabilities. A maritime red team may attempt to compromise a vessel's navigation system, gain control of cargo handling equipment, or intercept communications. The insights gained from red-team activities inform improvements to policies, controls, and training.

Blue Team refers to the defenders who monitor, detect, and respond to security incidents. In a maritime context, the blue team may include ship security officers, shore-based IT staff, and incident response specialists. Blue-team activities involve log analysis, threat hunting, and the continual refinement of security configurations.

Security Operations Center (SOC) is a dedicated facility where security analysts monitor alerts, investigate incidents, and coordinate responses. A maritime SOC may aggregate data from multiple vessels, ports, and offshore platforms, providing a unified view of the threat landscape. Effective SOC operations rely on automation, threat intelligence integration, and clear escalation procedures.

Log Management involves the collection, storage, and analysis of system logs. Logs from navigation equipment, communication devices, and access control systems can provide crucial evidence during investigations. Proper log management requires timestamp synchronisation, secure storage, and retention policies that comply with regulatory mandates.

Time Synchronisation ensures that all devices in a network share a common clock, typically via Network Time Protocol (NTP). Accurate timestamps are vital for correlating events across disparate maritime systems, such as matching a suspicious login attempt with a corresponding AIS message. Unsynchronised clocks can impede forensic analysis and obscure the true sequence of events.

Compliance denotes adherence to laws, regulations, standards, and contractual obligations. Maritime compliance obligations may include IMO cyber risk guidelines, GDPR, national data protection statutes, and industry-specific standards such as ISO/IEC 27001. Demonstrating compliance often involves audits, certifications, and documentation of security controls.

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving security processes. Maritime organisations adopting ISO/IEC 27001 can align their cyber risk management with best-practice controls and gain recognition from partners and regulators.

ISO/IEC 27017 offers guidance on information security controls for cloud services. As maritime operators increasingly migrate data analytics workloads to cloud platforms, understanding cloud-specific risks and applying appropriate safeguards becomes essential. Controls may address data encryption, identity management, and the segregation of tenant data.

ISO/IEC 27701 extends ISO/IEC 27001 to incorporate privacy information management, providing a framework for managing personal data. Shipping companies handling crew or passenger data can use ISO/IEC 27701 to demonstrate systematic privacy governance, supporting compliance with GDPR and other privacy regulations.

Business Continuity Plan (BCP) outlines procedures to keep essential operations running during disruptions, including cyber incidents. A maritime BCP may detail alternate communication channels, manual navigation procedures, and contingency staffing plans. Regular testing of the BCP, such as tabletop exercises, ensures readiness when a real event occurs.

Disaster Recovery (DR) focuses on restoring IT systems after a catastrophic failure. In the maritime sector, DR might involve recovering a ship's electronic chart display system from backup media, or re-establishing satellite connectivity after a cyber-induced outage. DR strategies must consider the limited physical access to shipboard hardware while at sea.

Physical Security protects hardware and infrastructure from theft, tampering, or sabotage. On a vessel, physical security measures include locked equipment cabinets, CCTV surveillance, and access-controlled areas for bridge consoles. Even the most robust cyber controls can be undermined if an attacker gains physical access to a device.

Insider Threat describes risk originating from individuals with legitimate access who misuse their privileges. In maritime environments, insiders may be crew members, contractors, or port employees. An insider could deliberately leak cargo data, introduce malicious software, or unintentionally cause a breach through poor security practices.

Social Engineering exploits human psychology to persuade victims to disclose credentials or perform actions that compromise security. Beyond phishing, social engineering in maritime contexts may involve phone calls impersonating a ship's charterer, convincing a crew member to install a "software update" that is actually malware.

Denial-of-Service (DoS) Attack aims to disrupt the availability of a service by overwhelming it with traffic. A DoS attack targeting a port's terminal management system could delay vessel berthing, increase turnaround time, and generate financial penalties. Distributed denial-of-service (DDoS) attacks, which leverage multiple compromised devices, are particularly potent.

Supply Chain Attack occurs when an adversary compromises a third-party vendor to infiltrate the target organisation. For maritime operators, a compromised navigation software vendor could deliver a malicious update that silently installs a backdoor on all ships using that software. Detecting supply-chain attacks often requires rigorous vendor risk assessments.

Root of Trust is a hardware or firmware component that establishes a secure foundation for a system's operation. Trusted Platform Modules (TPM) and secure boot mechanisms are examples of roots of trust that

verify the integrity of software before it runs. Deploying a root of trust on shipboard computers helps prevent tampering with critical boot processes.

Secure Boot ensures that only signed and verified firmware is loaded during system startup. In maritime vessels, secure boot can protect against boot-level malware that would otherwise be difficult to detect once the system is operational. Implementation may require coordination with equipment manufacturers to support signed firmware.

Digital Certificate is an electronic document that binds a public key to an entity's identity, verified by a Certificate Authority (CA). Certificates are used for establishing secure TLS connections, authenticating devices, and signing software updates. In maritime communications, certificates can verify that a ship's AIS transponder is genuine and authorised.

Public Key Infrastructure (PKI) provides the framework for creating, managing, distributing, and revoking digital certificates. A robust PKI enables encrypted communications between vessels and shore, supports mutual authentication, and facilitates secure software distribution. Managing PKI across a fleet requires careful planning to handle certificate lifecycles and revocation.

Key Management involves the generation, storage, rotation, and destruction of cryptographic keys. Poor key management can lead to compromised encryption, such as when a private key is stored unencrypted on a vessel's control system. Best practices include using hardware security modules (HSMs) and enforcing regular key rotation.

Hardware Security Module (HSM) is a tamper-resistant device that securely stores cryptographic keys and performs encryption/decryption operations. Deploying HSMs on ships can protect keys used for VPN tunnels, encrypted storage, and digital signatures, reducing the risk of key extraction by attackers with physical access.

Secure Configuration refers to the process of hardening systems by disabling unnecessary services, applying the principle of least privilege, and enforcing strong authentication. For maritime OT devices, secure configuration may involve turning off unused serial ports, enforcing strong passwords on SCADA consoles, and applying network segmentation.

Baseline Configuration is a documented, approved set of settings that defines the normal, secure state of a system. Establishing a baseline allows administrators to detect deviations that may indicate a compromise. Baselines should be version-controlled and regularly reviewed to incorporate new security patches and organisational changes.

Change Management governs how modifications to systems are proposed, reviewed, approved, and implemented. In a maritime context, change management ensures that updates to navigation software or firmware upgrades to engine control units are performed safely, with appropriate testing and rollback procedures.

Rollback Plan defines the steps to revert a system to a previous state if an update causes instability or a security issue. For a vessel's bridge computer, a rollback plan might involve restoring a previously validated image from secure storage, allowing the ship to continue navigation while the issue is investigated.

Audit Trail is a chronological record of system activities, including user actions, configuration changes, and security events. Maintaining an audit trail is essential for forensic investigations, compliance reporting, and accountability. Audit logs should be protected against tampering and stored in a manner that ensures integrity.

Pen Test Report summarises the findings of a penetration test, including identified vulnerabilities, exploitation steps, and remediation recommendations. For maritime stakeholders, a clear pen test report helps prioritise fixes, allocate resources, and demonstrate due diligence to regulators and insurers.

Risk Register is a living document that lists identified risks, their assessed likelihood and impact, mitigation measures, and owners. In maritime cyber risk management, the risk register may track threats such as "unauthorised remote access to engine control" and document the implementation of firewalls and MFA as mitigation.

Threat Modelling is a structured approach to identifying potential attack vectors, adversary capabilities, and system vulnerabilities. Common frameworks include STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege). Applying threat modelling to a ship's bridge network can reveal where authentication is weak or where data flows are unencrypted.

Compliance Audit is an independent assessment that verifies whether an organisation meets regulatory and contractual obligations. In the maritime sector, a compliance audit may evaluate adherence to IMO cyber risk guidelines, GDPR data protection requirements, and ISO/IEC 27001 security controls.

Incident Log captures details of a security incident, including detection time, actions taken, stakeholders involved, and lessons learned. Maintaining a thorough incident log supports continuous improvement, helps satisfy reporting obligations, and provides evidence for insurance claims.

Insurance Claim may be filed after a cyber incident that results in financial loss, operational disruption, or damage to assets. Maritime cyber insurance policies often require documented evidence of risk assessments, security controls, and incident response procedures. Proper documentation can expedite claim processing and reduce payout disputes.

Business Impact Analysis (BIA) evaluates the consequences of disruptions to critical processes. In maritime data analytics, a BIA might assess how loss of AIS data affects route planning, how compromised cargo data impacts customs clearance, and how downtime of a port's terminal management system affects revenue. Findings from the BIA drive prioritisation of recovery objectives.

Recovery Time Objective (RTO) defines the maximum acceptable duration to restore a service after a

disruption. For a ship's electronic chart system, the RTO might be set to 30 minutes, ensuring that navigation can resume quickly after a cyber incident. RTOs guide the design of backup solutions and recovery procedures.

Recovery Point Objective (RPO) specifies the maximum tolerable data loss measured in time. An RPO of one hour for cargo manifest data means that backups must be performed at least hourly, limiting the amount of data that could be lost in a breach. RPOs influence backup frequency and storage strategies.

Backup Strategy outlines how data is duplicated, where it is stored, and how it is protected. In maritime environments, backups may be stored on encrypted external drives, transmitted to secure cloud storage via satellite, or retained on-shore for regulatory compliance. Redundancy, encryption, and regular testing are essential components.

Cold Backup stores data offline, disconnected from the network, typically on physical media such as tapes or external hard drives. Cold backups are immune to ransomware attacks because they cannot be accessed remotely. However, they require manual handling to restore, which may be challenging for ships at sea.

Hot Backup maintains a real-time replica of operational data, enabling immediate failover. A hot backup of a ship's navigation database could allow seamless switchover if the primary system becomes compromised. Hot backups demand robust network connectivity and careful synchronization to avoid data inconsistency.

Data Masking replaces sensitive information with fictional but realistic values for use in testing or analytics. Maritime data analysts may mask crew names and passport numbers when working with real-world datasets to comply with privacy regulations while preserving analytical value.

Data Anonymisation removes personally identifiable information so that individuals cannot be re-identified. Anonymised AIS data can be shared with research institutions without violating privacy laws, enabling studies on traffic patterns while protecting vessel identities.

Data Governance Framework provides the structure for policies, standards, and procedures that manage data throughout its lifecycle. A maritime data governance framework might define data owners for cargo information, set quality standards for sensor readings, and prescribe security controls for data in transit.

Data Steward is an individual responsible for managing and ensuring the quality of a specific dataset. In a shipping company, a data steward might oversee the integrity of fuel consumption records, ensuring that they are accurate, secure, and compliant with reporting requirements.

Data Custodian handles the technical aspects of data storage, protection, and transmission. Custodians implement encryption, backup, and access controls as dictated by data owners and stewards. In maritime contexts, the IT department may act as the custodian for the vessel's performance monitoring database.

Data Owner holds ultimate accountability for a dataset, defining its purpose, usage, and protection level. The cargo manager could be the data owner for shipment manifests, determining who may view the data

and what retention policies apply.

Data Lifecycle describes the stages through which data passes, from creation and usage to archiving and destruction. Understanding the data lifecycle helps identify points where security controls are needed, such as encrypting data during transmission and securely wiping data from decommissioned devices.

Secure Erasure ensures that deleted data cannot be recovered, typically by overwriting storage media with random patterns. When a vessel retires an old navigation computer, secure erasure prevents residual data from being recovered by an adversary.

Privacy Impact Assessment (PIA) evaluates how personal data is collected, used, and protected, identifying privacy risks and mitigation strategies. Shipping companies conducting a PIA for a crew welfare app can uncover potential data leakage points and implement stronger access controls before deployment.

Data Subject Rights are the entitlements granted to individuals under privacy laws, such as the right to access, correct, or delete personal data. Crew members can request that their medical records be updated or removed, and the organisation must have processes to fulfil these requests within prescribed timeframes.

Data Processor is an entity that processes personal data on behalf of a data controller. A cloud service provider hosting crew payroll information acts as a data processor and must adhere to contractual obligations that ensure data protection and confidentiality.

Data Controller determines the purposes and means of processing personal data. In a maritime company, the human resources department typically acts as the data controller for employee records, deciding how data is stored, shared, and retained.

Data Breach Notification is the legal requirement to inform affected individuals and authorities about a breach. Under GDPR, a maritime operator must notify the supervisory authority within 72 hours of becoming aware of a breach that compromises crew personal data.

Secure Development Lifecycle (SDLC) integrates security activities into each phase of software development, from requirements gathering to maintenance. An SDLC for a vessel's fuel-management application would include threat modelling during design, code reviews during development, and regular security testing before deployment.

Static Application Security Testing (SAST) analyses source code for vulnerabilities without executing the program. SAST tools can detect hard-coded credentials, insecure API calls, and buffer overflows in maritime software before it reaches production.

Dynamic Application Security Testing (DAST) evaluates a running application for security weaknesses by sending malformed inputs and monitoring responses. DAST can uncover runtime issues such as improper input validation in a ship's cargo tracking portal.

Runtime Application Self-Protection (RASP) monitors an application's behavior during execution, detecting and blocking attacks in real time. Deploying RASP on a vessel's logistics management system can prevent injection attacks that attempt to alter shipment data.

Container Security addresses the protection of containerised applications, which are increasingly used for maritime data analytics. Security measures include scanning container images for known vulnerabilities, applying least-privilege policies, and isolating containers with appropriate runtime security controls.

Orchestration Platform Security focuses on securing tools such as Kubernetes that manage container deployments. In a maritime analytics platform, securing the orchestration layer prevents attackers from gaining control over the entire analytics pipeline.

Zero-Day Vulnerability is a security flaw that is unknown to the vendor and therefore has no available patch. Zero-day exploits targeting maritime navigation software can be especially dangerous because vessels may lack the ability to remediate quickly while at sea.

Threat Hunting is the proactive search for hidden threats within an environment, often using hypothesis-driven investigations. Maritime threat hunters may look for signs of lateral movement from the crew welfare network into the bridge network, using analytics to spot anomalous login patterns.

Security Information and Event Management (SIEM) aggregates logs, correlates events, and provides alerts for potential security incidents. A maritime SIEM can ingest data from shipboard firewalls, satellite communication logs, and port access control systems, offering a holistic view of the security posture.

Security Orchestration, Automation and Response (SOAR) automates repetitive security tasks, such as isolating compromised hosts, enriching alerts with