NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Doc Secure Controls Framework (SCF) version 2025.4
STRM Guidanc https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management
Focal Document URL: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/MSC-FAL.1-Circ.3-Rev.3.pd
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-scf-strm-general-imo-maritime-cyber-risk-management.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3	N/A	Elements of Cyber Risk Management	Functional	Not Related To	N/A	N/A	N/A	0	Nothing to map to
3.1	N/A	For the purpose of these Guidelines, cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and tolerating, terminating, transferring or treating it to an acceptable level, considering costs and benefits of actions taken by stakeholders.	Functional	Not Related To	N/A	N/A	N/A	0	Nothing to map to
3.2	N/A	The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyberthreats and risks. Safeguarding ships and ship-port interfacing systems from emerging threats should involve a range of controls that are continually evolving. Therefore, cyber resilient security features should be incorporated in the ship's equipment and systems at the design, manufacturing, integration, operation and maintenance stages.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	10	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	8	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	8	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	8	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	8	
3.3	N/A	Effective cyber risk management should start at the senior management level. Senior management should follow the relevant training and embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
3.4	N/A	One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal cybersecurity gaps in CBSs that can be addressed to achieve cyber resilience objectives through a risk-based approach. This risk-based approach is to evaluate the cyber risks, considering ship type and operational profile as well as onboard systems' complexity and connectivity, which will enable an organization to best apply its resources in the most cost-effective and efficient manner	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	8	
3.5	N/A	These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. The functional/technical cybersecurity controls listed under each of the functional elements represent the minimum controls that should be implemented. Additional cybersecurity controls may be considered depending on the evaluation of the identified cyber risks.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
3.5	N/A	These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. The functional/technical cybersecurity controls listed under each of the functional elements represent the minimum controls that should be implemented. Additional cybersecurity controls may be considered depending on the evaluation of the identified cyber risks.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
3.5	N/A	These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. The functional/technical cybersecurity controls listed under each of the functional elements represent the minimum controls that should be implemented. Additional cybersecurity controls may be considered depending on the evaluation of the identified cyber risks.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
3.5	N/A	These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. The functional/technical cybersecurity controls listed under each of the functional elements represent the minimum controls that should be implemented. Additional cybersecurity controls may be considered depending on the evaluation of the identified cyber risks.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
3.5.1	N/A	Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	8	
3.5.1	N/A	Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
3.5.1	N/A	Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
3.5.1	N/A	Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.5.1	N/A	Govern: Establish and monitor risk management strategy, expectations and policies. Define personnel roles and responsibilities for cyber risk management. Ensure business continuity, such as backup management and disaster recovery, and crisis management.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
3.5.1.1	N/A	Designate a person or entity accountable for the planning, resourcing and execution of cybersecurity activities.	Functional	Subset Of	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	10	
3.5.1.2	N/A	Ensure that the designated person or entity is given the necessary authority and support to fulfil their duties and that they have sufficient knowledge and expertise in cyber risk management.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	
3.5.1.2	N/A	Ensure that the designated person or entity is given the necessary authority and support to fulfil their duties and that they have sufficient knowledge and expertise in cyber risk management.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.5.1.2	N/A	Ensure that the designated person or entity is given the necessary authority and support to fulfil their duties and that they have sufficient knowledge and expertise in cyber risk management.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
3.5.1.2	N/A	Ensure that the designated person or entity is given the necessary authority and support to fulfil their duties and that they have sufficient knowledge and expertise in cyber risk management.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
3.5.2	N/A	Identify: Determine the current cyber risk to ships and ship/port interfaces	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
3.5.2.1	N/A	Identify the systems, assets, services, data and capabilities, interdependencies between safety critical systems (including the information flow) that, when disrupted, pose risks to ship operations, human safety, safety of the ship and/or a threat to the environment, including those related to the software and hardware supply chains	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
3.5.2.1	N/A	Identify the systems, assets, services, data and capabilities, interdependencies between safety critical systems (including the information flow) that, when disrupted, pose risks to ship operations, human safety, safety of the ship and/or a threat to the environment, including those related to the software and hardware supply chains	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	8	
3.5.2.1	N/A	Identify the systems, assets, services, data and capabilities, interdependencies between safety critical systems (including the information flow) that, when disrupted, pose risks to ship operations, human safety, safety of the ship and/or a threat to the environment, including those related to the software and hardware supply chains	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
3.5.2.2	N/A	Establish and maintain an inventory of digital systems on board the ship. These systems and assets could include the systems listed in paragraph 2.2.1 of these guidelines. Identify internal and external systems dependencies and network connections.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	8	
3.5.2.2	N/A	Establish and maintain an inventory of digital systems on board the ship. These systems and assets could include the systems listed in paragraph 2.2.1 of these guidelines. Identify internal and external systems dependencies and network connections.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
3.5.2.3	N/A	Carry out a risk assessment of those systems, services, assets, data and capabilities critical to ship operations, the sudden operational failure of which may result in hazardous situations. Identify cyber-related threats. Identify vulnerabilities to systems, services, assets, data and capabilities. Assess the likelihood and impact of a cyber incident on the safety, availability, integrity and confidentiality of those elements.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
3.5.2.3	N/A	Carry out a risk assessment of those systems, services, assets, data and capabilities critical to ship operations, the sudden operational failure of which may result in hazardous situations. Identify cyber-related threats. Identify vulnerabilities to systems, services, assets, data and capabilities. Assess the likelihood and impact of a cyber incident on the safety, availability, integrity and confidentiality of those elements.	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	3	
3.5.2.3	N/A	Carry out a risk assessment of those systems, services, assets, data and capabilities critical to ship operations, the sudden operational failure of which may result in hazardous situations. Identify cyber-related threats. Identify vulnerabilities to systems, services, assets, data and capabilities. Assess the likelihood and impact of a cyber incident on the safety, availability, integrity and confidentiality of those elements.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
3.5.2.3	N/A	Carry out a risk assessment of those systems, services, assets, data and capabilities critical to ship operations, the sudden operational failure of which may result in hazardous situations. Identify cyber-related threats. Identify vulnerabilities to systems, services, assets, data and capabilities. Assess the likelihood and impact of a cyber incident on the safety, availability, integrity and confidentiality of those elements.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
3.5.3	N/A	Protect: Implement risk control processes and measures to protect CBSs, and contingency planning to protect against a cyber incident and ensure business continuity of shipping operations, human safety, safety of the vessel and/or threat to the environment.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
3.5.3	N/A	Protect: Implement risk control processes and measures to protect CBSs, and contingency planning to protect against a cyber incident and ensure business continuity of shipping operations, human safety, safety of the vessel and/or threat to the environment.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
3.5.3.1	N/A	Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deactivate accounts for departing employees or users.	Functional	Subset Of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	10	
3.5.3.1	N/A	Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deactivate accounts for departing employees or users.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
3.5.3.1	N/A	Assign unique credentials for all users, separate user and privileged accounts, collect security devices and deactivate accounts for departing employees or users.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
3.5.3.2	N/A	Change all default passwords on all devices, enforce a strong password policy and consider establishing other user account access control management measures to safeguard against malicious attempts such as brute force attacks, phishing, etc. Use multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
3.5.3.2	N/A	Change all default passwords on all devices, enforce a strong password policy and consider establishing other user account access control management measures to safeguard against malicious attempts such as brute force attacks, phishing, etc. Use multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
3.5.3.2	N/A	Change all default passwords on all devices, enforce a strong password policy and consider establishing other user account access control management measures to safeguard against malicious attempts such as brute force attacks, phishing, etc. Use multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
3.5.3.2	N/A	Change all default passwords on all devices, enforce a strong password policy and consider establishing other user account access control management measures to safeguard against malicious attempts such as brute force attacks, phishing, etc. Use multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	8	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	5	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.	3	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
3.5.3.3	N/A	Limit exploitable services on the Internet, establish a hardware and software approval process, collect and securely store logs for intrusion detection and incident response, and segment OT device networks from IT networks. Ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
3.5.3.4	N/A	Implement security measures (such as firewall or antivirus) for any ship digital systems and devices that have access to the Internet or the company's intranet, or any interaction with third party or landside network and information systems, particularly those of ship/port interfaces. Implement policies and procedures regarding the use of cryptography.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
3.5.3.4	N/A	Implement security measures (such as firewall or antivirus) for any ship digital systems and devices that have access to the Internet or the company's intranet, or any interaction with third party or landside network and information systems, particularly those of ship/port interfaces. Implement policies and procedures regarding the use of cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
3.5.3.4	N/A	Implement security measures (such as firewall or antivirus) for any ship digital systems and devices that have access to the Internet or the company's intranet, or any interaction with third party or landside network and information systems, particularly those of ship/port interfaces. Implement policies and procedures regarding the use of cryptography.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
3.5.3.5	N/A	Establish controls to protect systems from the use of unauthorized removable media.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
3.5.3.5	N/A	Establish controls to protect systems from the use of unauthorized removable media.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
3.5.3.6	N/A	Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises	Functional	Subset Of	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	10	
3.5.3.6	N/A	Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	8	
3.5.3.6	N/A	Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
3.5.3.6	N/A	Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises	Functional	Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity and data protection training that reinforce training objectives.	5	
3.5.3.6	N/A	Mandate annual basic cybersecurity training for all employees and OT-specific cybersecurity training for OT users, and cybersecurity familiarization to all crew members upon engagement on board the ship. This training for all employees and OT users should include elements on cyber hygiene, the recognition and detection of an ongoing cyber incident, as well as response and recovery. Knowledge on cybersecurity should occasionally be tested, for example through drills and exercises	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
3.5.3.7	N/A	Perform regular system backups, software updates, and develop and maintain incident response (IR) plans.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
3.5.3.7	N/A	Perform regular system backups, software updates, and develop and maintain incident response (IR) plans.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
3.5.3.7	N/A	Perform regular system backups, software updates, and develop and maintain incident response (IR) plans.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	8	
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	3	
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	8	
3.5.3.8	N/A	Establish policies on software and hardware supply chain security for those systems and assets that have been identified as critical.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
3.5.3.9	N/A	Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	8	
3.5.3.9	N/A	Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.5.3.9	N/A	Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
3.5.3.9	N/A	Establish policies and procedures to assess the effectiveness of cyber risk management measures, such as audits, and to periodically review and update these measures.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	8	
3.5.4	N/A	Detect: Develop, implement and practise activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
3.5.4	N/A	Detect: Develop, implement and practise activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.5.4	N/A	Detect: Develop, implement and practise activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
3.5.4	N/A	Detect: Develop, implement and practise activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.5.4.1	N/A	Maintain a list of relevant threats, threat actor tactics, techniques and procedures and actively monitor systems for those threats.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
3.5.4.1	N/A	Maintain a list of relevant threats, threat actor tactics, techniques and procedures and actively monitor systems for those threats.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
3.5.4.1	N/A	Maintain a list of relevant threats, threat actor tactics, techniques and procedures and actively monitor systems for those threats.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	
3.5.4.2	N/A	Annual basic cybersecurity training for all employees should include training on recognizing and detecting an ongoing cyber incident.	Functional	Subset Of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
3.5.4.2	N/A	Annual basic cybersecurity training for all employees should include training on recognizing and detecting an ongoing cyber incident.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
3.5.4.2	N/A	Annual basic cybersecurity training for all employees should include training on recognizing and detecting an ongoing cyber incident.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
3.5.5	N/A	Respond: Develop, implement and practise activities and plans to provide resilience and to restore systems necessary for shipping and ship-port operations or services impaired due to a cyber incident. Implement appropriate measures to minimize the effect of a detected cyber incident to other parts of ship systems.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
3.5.5	N/A	Respond: Develop, implement and practise activities and plans to provide resilience and to restore systems necessary for shipping and ship-port operations or services impaired due to a cyber incident. Implement appropriate measures to minimize the effect of a detected cyber incident to other parts of ship systems.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
3.5.5	N/A	Respond: Develop, implement and practise activities and plans to provide resilience and to restore systems necessary for shipping and ship-port operations or services impaired due to a cyber incident. Implement appropriate measures to minimize the effect of a detected cyber incident to other parts of ship systems.	Functional	Subset Of	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	10	
3.5.5.1	N/A	Report incidents to necessary parties within required time frames as defined by the Administration.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
3.5.5.1	N/A	Report incidents to necessary parties within required time frames as defined by the Administration.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
3.5.5.2	N/A	Records of cyber incidents should be kept.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
3.5.5.2	N/A	Records of cyber incidents should be kept.	Functional	Subset Of	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
3.5.5.3	N/A	Annual basic cybersecurity training for all employees should include training on responding to a cyber incident.	Functional	Subset Of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
3.5.5.3	N/A	Annual basic cybersecurity training for all employees should include training on responding to a cyber incident.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
3.5.6	N/A	Recover: Identify and implement measures to restore onboard CBS including networks necessary for shipping operations impacted by a cyber incident.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.5.6	N/A	Recover: Identify and implement measures to restore onboard CBS including networks necessary for shipping operations impacted by a cyber incident.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
3.5.6.1	N/A	Develop, maintain and implement strategies for the recovery and reinstatement of essential business or mission critical assets or systems that might be impacted by a cyber incident.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.5.6.1	N/A	Develop, maintain and implement strategies for the recovery and reinstatement of essential business or mission critical assets or systems that might be impacted by a cyber incident.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
3.5.6.1	N/A	Develop, maintain and implement strategies for the recovery and reinstatement of essential business or mission critical assets or systems that might be impacted by a cyber incident.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	8	
3.5.6.2	N/A	Annual basic cybersecurity training for all employees should include training on recovering from a cyber incident.	Functional	Subset Of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.5.6.2	N/A	Annual basic cybersecurity training for all employees should include training on recovering from a cyber incident.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
3.5.6.3	N/A	Carry out root cause analysis of cyber incidents, with the objective of resolving underlying issues and vulnerabilities to prevent similar recurrence.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	
3.5.6.3	N/A	Carry out root cause analysis of cyber incidents, with the objective of resolving underlying issues and vulnerabilities to prevent similar recurrence.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
3.6	N/A	These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms. Any documents, or sections of documents, developed to satisfy these functional elements should be protected by procedures aimed at preventing unauthorized access, deletion, destruction or amendment.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	
3.7	N/A	Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity and data protection principles into Business As Usual (BAU) practices through executive leadership involvement.	8	
3.8	N/A	Implementation of cyber resilient equipment and systems is to be considered. As part of technical measures, equipment and systems should be designed and tested as per international standards and guidance to assure cyber resilience on board ships.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
3.8	N/A	Implementation of cyber resilient equipment and systems is to be considered. As part of technical measures, equipment and systems should be designed and tested as per international standards and guidance to assure cyber resilience on board ships.	Functional	Subset Of	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	10	