Digital Container Shipping Association

DCSA Implementation Guide for Cyber Security on Vessels v1.0

10/03/2020

Glossary

BIMCO	Baltic and International Maritime Council
CCTV	Closed - Circuit Television
CISO	Chief Information and Security Officer
CMDB	Configuration Management Database
CRM	Cyber Risk Management
CSA	Cyber Security Assessment
CSO	Company Security Officer
CSP	Cyber Security Plan
CySO	Cyber Security Officer
DOC	Document of Compliance
DPA	Designated Person Ashore
ECDIS	Electronic Chart Display and Information System
FISMA	Federal Information Security Management Act
IDS	Intrusion Detection System
IMO	International Maritime Organisation
IPS	Intrusion Prevention System
ISM	International Safety Management
ISPS	International Ship and Port Facility Security
IT	Information Technology
MARPOL	Maritime Pollution
MSC	Maritime Safety Committee
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OT	Operational Technology
PLC	Programmable logic Controller
PMR	Private Mobile Radio
POC	Proof of Concept
RMF	Risk Management Framework
SBAR	Situation, Background, Assessment and Recommendation
SIEM	Security Information and Event Management
SMS	Safety Management System
SOLAS	Safety of Life at Sea
SSA	Ship Security Assessment
SSO	Ship Security Officer
SSP	Ship Security Plan
STCW	The International Convention on Standards of Training and Watchkeeping for seafarers

Introduction

Introduction

The rapid evolution in the use of, and reliance upon, digital (computer-based) and communication technologies, as well as the advances in automation and the potential for integration of multiple electronic systems supporting management functions and business applications, increases the importance of addressing inherent vulnerabilities. It is therefore vital that vessel owners, operators and masters understand and implement appropriate and proportionate measures to address the resilience and cyber security issues that arise. Only by doing so can they fully meet their responsibilities for the secure and safe operation of their vessels.

Recommendations relating to these aspects are therefore detailed throughout the implementation guideline where relevant. With the exception of any vessel/port interface, it is not the purpose of this implementation guideline to consider the cyber security of the ports and port facilities to which the ISPS Code also applies.

This DCSA implementation guideline is aimed at assisting those companies with the responsibility of implementing and ensuring compliance with the BIMCO guidelines for cyber security on-board vessels. As a guideline, it does not set out specific technical or configuration standards for vessel systems, but instead provides a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of the vessel, the crew, or the cargo. Lastly it is aligned with the IMO Resolution MSC.428(98) compliance.

Scope Implementation Guideline

The scope of this document is aimed at vessel owners, but vessels under management could utilise this framework in order to verify cyber security controls on-board vessels.

1. DCSA implementation guidelines propose a cyber security management framework for vessels whether at sea, moored or berthed. Advocating a coherent vessel, or fleet-wide approach.
2. It is intended to complement the ship security standards and their respective requirements, by providing additional guidance on the cyber-related aspects of the security measures set out.
3. This implementation framework adheres to the BIMCO guidelines rather than any applicable flag legislation or specific principles to help promote good practice.
4. The target audience is **Cyber Security leads** who will be responsible for fleet-wide cyber security on-board vessels.

In scope - Vessels which may include:

- Information Technology (IT) such as computers, electronic manuals, networks. and applications.
- Operational Technology (OT) such as engine control, ECDIS, on-board measurement and control systems, PLCs and remote support for engines.

Out of scope - Shore-based information assets which are typically:

- All enterprise IT that isn't physically located on-board a vessel.

Audience

In addition to the cyber security lead this implementation guideline is intended for use by those with responsibility for protecting the vessel (both when underway and when docked or berthed), persons, cargo, cargo transport units and vessel's stores from the risks of a cyber security incident. As such, the secondary audience for this document is:

- Board members of organisations with one or more Container Vessels
- The Captain / Master
- Chief Officer
- Chief Engineer
- Those applicable roles that are responsible for the day-to-day operation of maritime information technology (IT), operational technology (OT) and communications systems.

It will also be of interest and relevance to those individuals involved in:

- The financial and operational management of a vessel or fleet;
- Insuring vessels and their cargoes;
- Contractual arrangements with third parties;
- Determining policies relating to acceptable staff behaviour;
- The specification, design, construction and maintenance of vessels;
- The specification, design, development, integration, commissioning, operation and maintenance of maritime systems, including associated software and technologies; and
- Management of specific security tasks, including incident response and the handling of security breaches.

Cyber Security and the Purpose of this Guideline

Cyber security is not just about preventing hackers gaining access to systems and information, potentially resulting in loss of confidentiality and/or control. It also addresses the maintenance of Confidentiality, Integrity and Availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems.

To achieve this, consideration needs to be given to not only protecting vessel systems from physical attack, force majeure events, etc., but also to ensuring the design of the systems and supporting processes is resilient and that appropriate reversionary modes are available in the event of compromise. Personnel security aspects are also important. The insider threat from shore-based or shipboard individuals who decide to behave in a malicious manner, or the untrained user that makes errors cannot be ignored. Ship owners and operators need to understand cyber security and promote awareness of this subject to their stakeholders, including their shipboard personnel.

This implementation guideline is intended to be used as an integral part of a company's or ship's overall risk management system and subsequent business planning. To ensure that the cyber security of the ship, or fleet, is of a sufficient standard that vessel owners can demonstrate that their Safety Management System has addressed all cyber considerations laid down in the BIMCO guidelines.

Cyber Security Roles

One key area that is vital for successful implementation of the BIMCO guidelines is the correct identification, preparation and allocation of cyber security roles in relation to cyber security on-board vessels.

Master

Hi, I'm Michael and I'm the Captain on this vessel

For a Safety Management System to be effective , it should be short, to the point and with clear steps.

My Company's Cyber Security Management Plan based on the DCSA Cyber Security Guidelines gave us a practical and understandable plan which could be implemented on-board.

Navigation Officer

Hi, I'm Neil and I'm the Navigation Officer on this vessel

Although ECDIS is an important milestone for shipping, failure of this system due to a cyber attack will impact the safe operation of the vessel. Using the DCSA Cyber Security Implementation Guidelines to set up our Cyber Security Management Plan, any cyber incident related to our navigation equipment can be detected, responded to and recovered from.

Designated Person Ashore

Hi, I'm Daisy and I'm the Designated Person Ashore.

Preparing Safety Management Systems is a quite difficult job. I have noticed that plans and procedures are often not read by the vessel's crew and just stored. Preparing a Cyber Security Management Plan requires a solid framework with clear and understandable procedures. The DCSA guideline assists with preparation and promotes understanding.

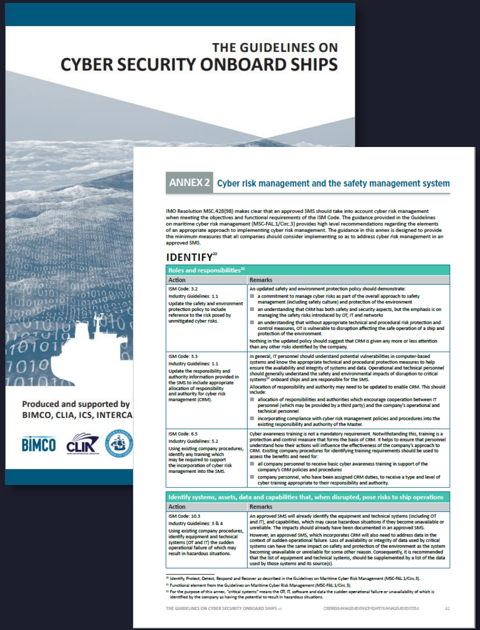
Introducing the NIST Cyber Security Framework

CYBER SECURITY FRAMEWORK

1. IDENTIFY	2. PROTECT	3. DETECT	4. RESPOND	5. RECOVER
1.1 Asset Management	2.1 Identity Management and Access Control	3.1 Anomalies and Events	4.1 Response Planning	5.1 Recovery Planning
1.2 Business Environment	2.2 Awareness and Training	3.2 Security Continuous Monitoring	4.2 Communications	5.2 Improvements
1.3 Governance	2.3 Data Security	3.3 Detection Processes	4.3 Analysis	5.3 Communications
1.4 Risk Assessment	2.4 Information Protection Processes and Procedures		4.4 Mitigation	
1.5 Risk Management Strategy	2.5 Maintenance		4.5 Improvements	
1.6 Supply Chain Risk Management	2.6 Protective Technology			

DCSA Approach

From the BIMCO Guidelines to NIST Controls



THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCA

ANNEX 2 Cyber risk management and the safety management system

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

IDENTIFY[20]

Roles and responsibilities[21]

Action	Remarks
ISM Code: 3.2 Industry Guidelines: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Industry Guidelines: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[22] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

Action	Remarks
ISM Code: 10.3 Industry Guidelines: 3 & 4 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).

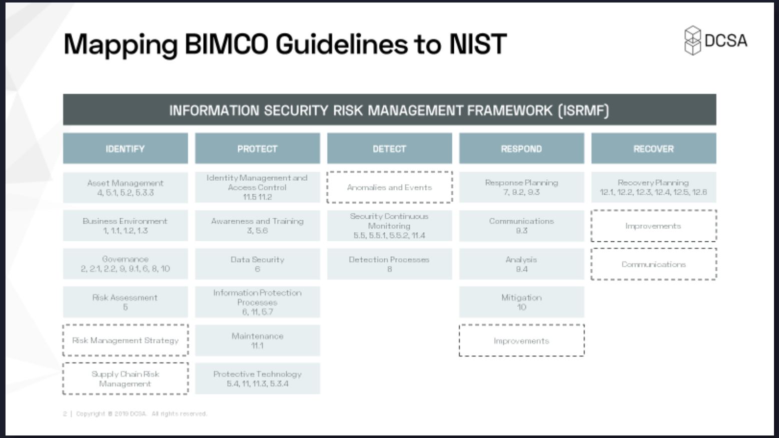
[20] Identify, Protect, Detect, Respond and Recover as described in the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[21] Functional element from the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[22] For the purpose of this annex, "critical systems" means the OT, IT, software and data the sudden operational failure or unavailability of which is identified by the company as having the potential to result in hazardous situations.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS v3 CYBER RISK MANAGEMENT AND THE SAFETY MANAGEMENT SYSTEM 42

BIMCO Guidelines annex 2 is divided into logical themes according to normal Cyber Security practice.



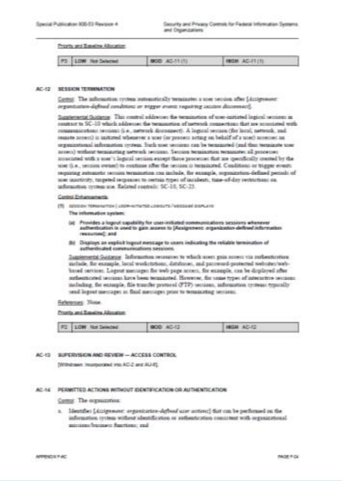
Mapping BIMCO Guidelines to NIST

INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK (ISRMF)

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management 4, 5.1, 5.2, 5.3.3	Identity Management and Access Control 11.5 11.2	Anomalies and Events	Response Planning 7, 9.2, 9.3	Recovery Planning 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
Business Environment 1, 1.1, 1.2, 1.3	Awareness and Training 3, 5.6	Security Continuous Monitoring 5.5, 5.5.1, 5.5.2, 11.4	Communications 9.3	Improvements
Governance 2, 2.1, 2.2, 9, 9.1, 6, 8, 10	Data Security 6	Detection Processes 8	Analysis 9.4	Communications
Risk Assessment 5	Information Protection Processes 6, 11, 5.7		Mitigation 10	
Risk Management Strategy	Maintenance 11.1		Improvements	
Supply Chain Risk Management	Protective Technology 5.4, 11, 11.3, 5.3.4			

2 | Copyright © 2019 DCSA. All rights reserved.

Each identified theme is mapped into the NIST framework to ensure that all parts are covered.



Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

Priority and Baseline Allocation:

P3	LOW Not Selected	MOD AC-11 (1)	HIGH AC-11 (1)

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

References: None.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD AC-12	HIGH AC-12

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

a. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

APPENDIX F-AC PAGE F-24

NIST Controls* are listed for each themes to allow each carrier to pursue their desired maturity level.

* ISO/IEC and COBIT controls also available

Dividing BIMCO Annex 2 into Logical Themes

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCA

ANNEX 2 Cyber risk management and the safety management system

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

IDENTIFY[20]

Roles and responsibilities[21]

Action	Remarks
ISM Code: 3.2 Industry Guidelines: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Industry Guidelines: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[22] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

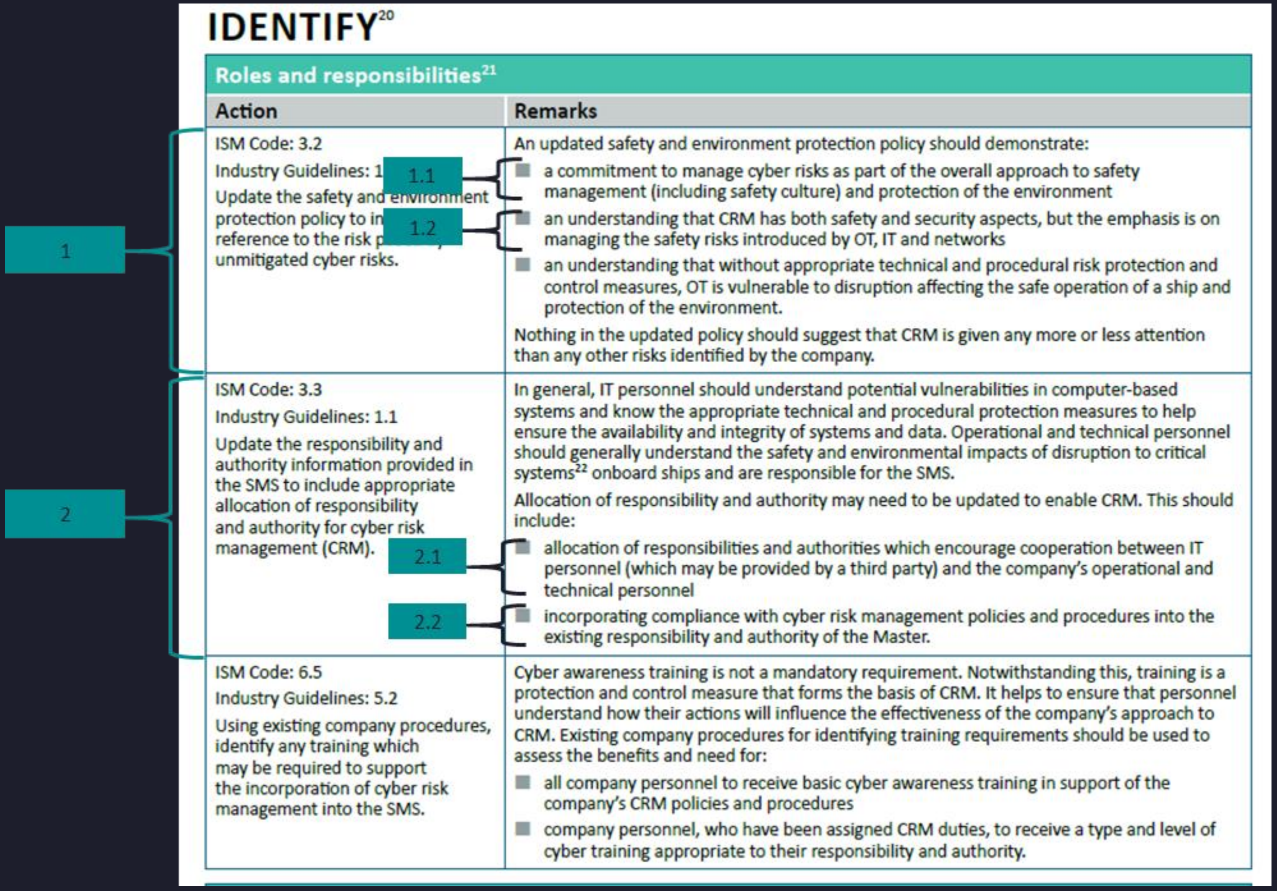
Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

Action	Remarks
ISM Code: 10.3 Industry Guidelines: 3 & 4 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).

[20] Identify, Protect, Detect, Respond and Recover as described in the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[21] Functional element from the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[22] For the purpose of this annex, "critical systems" means the OT, IT, software and data the sudden operational failure or unavailability of which is identified by the company as having the potential to result in hazardous situations.


1
1.1
1.2
2
2.1
2.2

IDENTIFY[20]

Roles and responsibilities[21]

Action	Remarks
ISM Code: 3.2 Industry Guidelines: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Industry Guidelines: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[22] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

Mapping BIMCO Guidelines to NIST

dcsa

CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management 4, 5.1, 5.2, 5.3.3	Identity Management and Access Control 11.5 11.2	Anomalies and Events	Response Planning 7, 9.2, 9.3	Recovery Planning 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
Business Environment 1, 1.1, 1.2, 1.3	Awareness and Training 3, 5.6	Security Continuous Monitoring 5.5, 5.5.1, 5.5.2, 11.4	Communications 9.3	Improvements
Governance 2, 2.1, 2.2, 9, 9.1, 6, 8, 10	Data Security 6	Detection Processes 8	Analysis 9.4	Communications
Risk Assessment 5	Information Protection Processes 6, 11, 5.7		Mitigation 10	
Risk Management Strategy	Maintenance 11.1		Improvements	
Supply Chain Risk Management	Protective Technology 5.4, 11, 11.3, 5.3.4			

1. Identify

CYBER SECURITY FRAMEWORK				
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

1. Identify

MAERSK
MAERSK
MAERSK
MAERSK
MAERSK
MAERSK SEALAND
MAERSK
EVERGREEN

1.1 Asset Management

1.1 Asset Management

1.1.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 4 • 5.1 • 5.2 • 5.3.3	ID.AM-1: Physical devices and systems within the organisation are inventoried.	CM-8, PM-5
	ID.AM-2: Software platforms and applications within the organisation are inventoried.	CM-8, PM-5
	ID.AM-3: organisational communication and data flows are mapped.	AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued.	AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	CP-2, RA-2, SA-14, SC-6
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	CP-2, PS-7, PM-1

1.1 Asset Management

1.1.2 Explanation

EXPLANATION

The vessel may from a cyber security perspective, be considered as a 'system of systems', operated in a contained environment with external communications interfaces. The size and complexity of this system of systems will vary between vessels and DCSA member firms. In order to effectively manage risks against this system of systems, vessels must have an adequate understanding of what assets are held on-board as well as how critical those assets are. (Asset lists / inventories are more than likely already in place - particularly with regards to systems that are critical for on-board safety).

For the purposes of developing appropriate and proportionate cyber security measures, each of the IT or OT systems may be located in, or directly related to one of the following categories: (Please note that this list is not exhaustive)

a) **Communications –** systems provided for internal, vessel-to-shore and vessel-to-vessel communications. These may include remote monitoring systems such as voyage data recorders and systems that monitor the performance of the vessels subsystems. Such systems often connect to OT and navigation systems before the data is communicated often via satellite.

b) **Navigation Systems –** systems that are either directly for or provided in support of ship navigation.

c) **Plant Systems –** systems used for monitoring and control of any machinery and plant associated with the general operation of the vessel, not covered in other categories.

d) **Safety Systems –** systems used to maintain the integrity, safety and/or security of the ship and its cargo.

e) **Cargo Systems –** systems used to monitor and manage cargo directly.

f) **Crew Access Systems –** any systems provided for passenger/crew interaction that are not related to ship operations or passenger/crew management.

There should be an appropriate register to record all assets (including hardware and software), ownership, location, criticality and version numbering.

1.1 Asset Management

1.1.3 Implementation

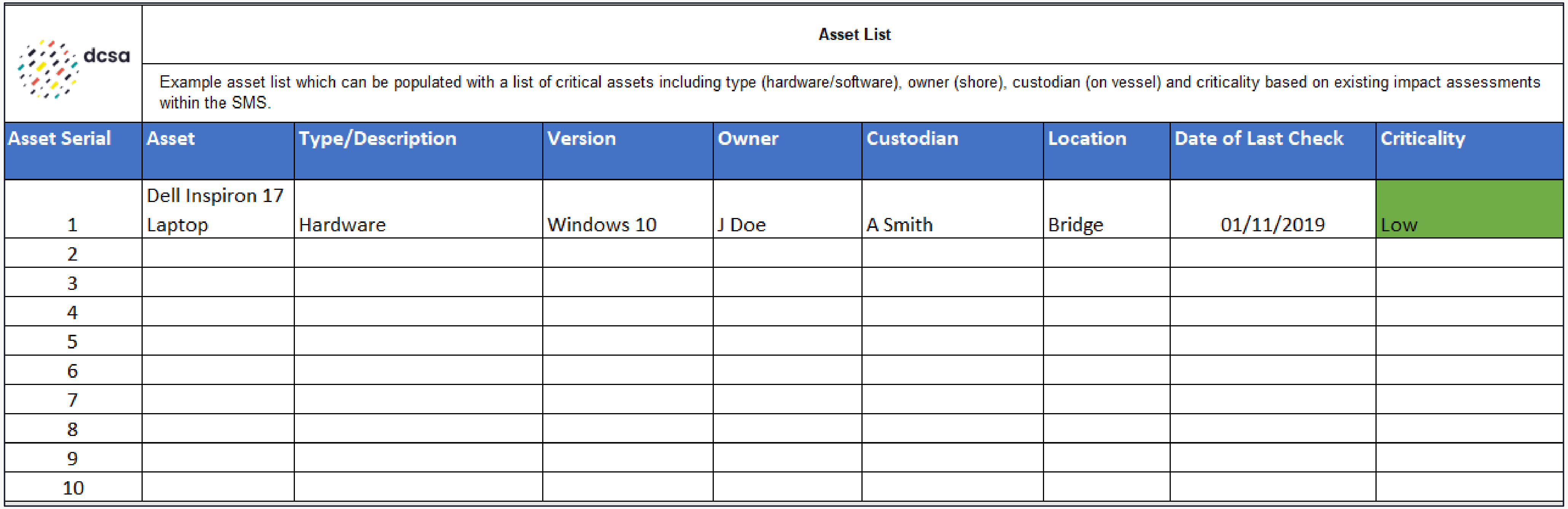
GUIDELINE
Ensure that all critical hardware devices within the organisation of the vessel are inventoried (BIMCO 5.1). This should form part of an asset lifecycle management process which documents the procurement or creation, processing, storage, transmission, deletion and destruction activities. This lifecycle should be documented in an asset register. An example is shown at 1.1.4.
The inventory should be accurate and kept up to date. There should be a process to review assets against the inventory to ensure that they match, this can be done on a periodic basis and incorporated into the SMS.
The asset inventory should also include all information assets. It is also important that version numbering of assets is recorded. An accurate and up to date configuration management database (CMDB) provides s good example of this. Register headings to use could include: • Serial number • Asset type (hardware/software) • Asset name • Asset owner • Version number • Location • Date of last review • Criticality (low, medium, high, safety critical)
Confirm that procedures exist for maintenance of this inventory when software controlled by the company is updated or changed (Bimco 5.2.2.). This can be achieved by ensuring that the asset inventory / CMDB is owned by a role with responsibility for asset inventory procedures. Everything should be included in the existing Safety Equipment Maintenance Plan under the three main conventions: Safety of Life at Sea (SOLAS), Standards for Training and Certification for Watchkeeping (STCW) and Maritime Pollution (MARPOL).

1.1Sample Asset List

1.1.4 Asset List

This page shows an example asset list. The headings are recommended in order to ensure that any asset which requires protection from cyber risks is identified, recorded and managed.

This can be done as part of, or in parallel with existing asset inventories, depending on company appetite.



Asset List

Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.

Asset Serial	Asset	Type/Description	Version	Owner	Custodian	Location	Date of Last Check	Criticality
1	Dell Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

1.2 Business Environment

1.2 Business Environment

- 1.2.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 1 • 1.1 • 1.2 • 1.3	ID.BE-1: The organisation's role in the supply chain is identified and communicated.	CP-2, SA-12
	ID.BE-2: The organisation's place in critical infrastructure and its industry sector is identified and communicated.	PM-8
	ID.BE-3: Priorities for organisational mission, objectives, and activities are established and communicated.	PM-11, SA-14
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).	CP-2, CP-11, SA-13, SA-14

1.2 Business Environment

- 1.2.2 Explanation

EXPLANATION

Traditionally, the business environment would focus on the business and information security factors that may affect this. Within this implementation guideline, the focus for the business environment is the specifics concerning operating vessels whilst reducing cyber risks on-board.

There are two critical areas which must be protected within the business environment on-board vessels:

- **Safety**
- **Operations**

This is applicable for vessels whether underway, moored or berthed.

Safety: Whilst the SMS is focused on conventional threats to safety on-board vessels, safety risks arising from cyber risks must also be captured in order that cyber-specific security controls can be implemented and monitored for effectiveness. An example of this would be if the availability of a piece of safety critical equipment was compromised due to an event such as malware, then this would have a significant impact on the ability of the vessel to operate safely.

Operations: This is focused on enabling the vessel to carry out its primary business function which is the timely and efficient delivery of cargo to the correct destination. Again, risks to any of the assets on-board that enable this process such as navigation systems, cargo handling systems or OT for engine management should be identified so that they can be subsequently dealt with.

1.2 Business Environment

- 1.2.3 Implementation

GUIDANCE
The vessel should be included in a process which defines mission/business processes with consideration for information security and the resulting risk to organisational operations, organisational assets, individuals, other organisations, and safety.
This process should determine information protection needs arising from the defined mission / business processes and revises the processes as necessary, until achievable protection and safety needs are obtained.
Ensure that the vessel's safety policy provides a safe and healthy environment on-board, safe working conditions for crew, safe equipment and systems of works by ensuring cyber risks are identified and mitigated. • Ensures safe and healthy working conditions on-board vessels • Establishes safeguards against all identified risks • There is a process to regularly monitor the performance and safety of vessels equipment • There is a process to monitor the performance and training level of sea-based personnel • Vessels and crews should be supplied with the necessary resources, information, training, and supervision in order to operate within the business environment safely The Quality, health, safety and environment protection policy should be updated to address: • Commitment to manage cyber risks • Understanding the importance of managing safety risks introduced by OT, IT and networks • Understanding that without appropriate control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment
There should be recognition that without appropriate technical and procedural risk protection control measures, and the close cooperation of crews; the health, safety and environmental protection cannot be improved. Rendering both IT and OT vulnerable to disruption. Thus, the company expects compliance from seafarers serving on-board vessels with safety procedures and instructions, to use PPE, take safety precautions as required, cooperate with the heads of their departments and Master, and to report anything they consider as hazardous for the safety of the vessel and crew. The upcoming regulation of Cyber Security Plan (ref IMO Resolution MSC.428(98)should be communicated to the vessel's crew.

1.3 Governance

1.3 Governance

- 1.3.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 2 • 2.1 • 2.2 • 6 • 8 • 9 • 9.1 • 10	ID.GV-1: organisational cybersecurity policy is established and communicated.	-1 controls from all security control families
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	PS-7, PM-1, PM-2
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy.	-1 controls from all security control families
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

1.3 Governance

- 1.3.2 Explanation

EXPLANATION

The BIMCO guidelines govern the establishment and implementation of cyber security practices on-board vessels. These guidelines provide high-level recommendations for maritime cyber risk management including defining responsibilities for cyber security, key information security roles and responsibilities, plus the identification and implementation of relevant information security controls.

It is envisaged that most if not all vessels will already be under a governance structure, particularly with regards to the business environment objectives of securing safety and continuation of operations. However, the specific challenges of introducing cyber security on-board vessels may require that additional governance considerations be taken into account, such as additional roles and responsibilities. Mapping additional governance to existing governance structures would assist a smooth transition. One example would be the creation of a Cyber Security Officer (CySO) role, possibly incorporated in the Ship’s Security officer (SSO) role.

The Maritime Security Regulations place legal requirements on the Company of a ship covered by the SOLAS Convention to put in place a Company Security Officer (CSO), who is responsible on behalf of the Company for preparation of the SSA and CSA. Section 8 of the ISPS Code requires the SSA to encompass the ship's radio and telecommunications systems, including computer systems and networks. The Company should ensure appropriate governance arrangements are in place regarding the roles and duties of the CSO and the CySO and that these are incorporated into existing governance structures.

Whilst this DCSA guideline will be describe additional roles and responsibilities, these will be functional and not organisational. This will enable companies to put these roles and responsibilities where they fit best for each company whilst also taking into account considerations such as number of vessels, araciality of resources and size.

1.3 Governance

- 1.3.3 Implementation

GUIDANCE
There should be a defined role on-board each vessel who owns the responsibility for cyber security on-board that vessel. The Security Officer described in this control is an organisational official. The role should be formally defined with a list of responsibilities that the role holder is trained and resourced to carry out.
Carriers should appoint a suitably qualified role / roles to lead the implementation of these guidelines. They must be able to identify cyber security gaps, implementation requirements and dependencies, as well as existing processes that can support these needs. Security-related aspects of the capital planning and investment control process.
There must be a solid governance framework in place to ensure that any cyber security policies, standards or processes are incorporated into existing governance frameworks to ensure that they work in support of existing systems and are not isolated efforts.
It may also be useful for carriers to create some form of "Cyber Security on-board Vessels" review team. Given the impacts on safety and operations, the complex technological landscape on-board a vessel and difficulties in initially delineating cyber security responsibilities between vessels and on-shore enterprise security, creating a review function with stakeholders from areas such as Safety, Enterprise Risk, Maritime Operations, IT Operations and Compliance would be beneficial to carriers at the start of this process.

1.3 Governance

- 1.3.4 Functional Roles and Responsibilities

Designated Person Ashore (DPA)

The DPA will under normal circumstances be the Cyber Security Lead officer of a carrier and will cooperate with the CISO. They are responsible for implementing and maintaining the Cyber Security Framework fleetwide and will have functional responsibility for Cyber Security roles on-board vessels.

Key Responsibilities

- Develop and manage a cyber security program that follows BIMCO as an industry standard
- Facilitate communication with the senior management
- Mediate disputes related to policies and standards
- Facilitate development of cyber security awareness training and awareness
- Provide relevant reporting to the senior management
- Initiate yearly review of the DOC

If this person is also the CSO it is also his responsibility to ensure ISPS compliance

Where the Company makes extensive use of contract personnel, the CSO should ensure appropriate measures are used for the secure procurement of contracting personnel, which includes appropriate screening or background checks. These checks should also be in place for staff employed through other mechanisms.

1.3 Governance

- 1.3.5 Functional Roles and Responsibilities

Cyber Security Officer (CySO)

Depending on the size or nature of the ship and/or fleet, the CySO role may be located on-board the ship, for example a vessel sailing on the high seas, or shore-based for ships that routinely operate either solely in international waters or working predefined routes between specific ports, or where a suitable resource is not available on-board. The CySO is responsible for all security aspects of cyber-enabled systems on the ship, including the IT, OT and communications systems.

NOTE: Where the ship operates both within national waters and in foreign waters, including the high seas, the CySO should understand the jurisdiction issues regarding law enforcement and cyber security incidents. however the issue of jurisdiction is a complex area for cyber security and maritime offences and expert legal advice should be sought in the event of an incident. Each organization should have an internal incident reporting process.

Key Responsibilities:

- Coordinating with the Company security officer (CSO) on aspects relating to physical, personnel and process security; and
- Ensuring the development, periodic review and maintenance of the CSA/CSP; and
- Implementing and exercising the CSP.

Where the CySO has insufficient knowledge of all cyber security issues and solutions, they should seek specialist cyber security advice from an appropriate professional source.

Note: The professional source may be provided by the Company or provided as a professional support contract arranged by the Company.

The CySO should maintain awareness of legal and regulatory changes that could affect the cyber security of ship assets and where necessary, adjust policies, processes and procedures to comply with those changes.

Note: The awareness of legal and regulatory changes may be monitored by the Company or provided through a professional support contract arranged by the Company, to be delivered to the CySO as a periodic update.

1.4 Risk Assessment

1.4 Risk Assessment

- 1.4.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented.	RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified.	RA-2, RA-3, SA-14, PM-9, PM-11
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized.	PM-4, PM-9

1.4 Risk Assessment

- 1.4.2 Explanation

EXPLANATION

Conducting a Risk Assessment is one of the most important aspects of cyber security. This is because the process should formally identify the information assets which are important to the company in achieving its business aims, the criticality of those assets, the threats against them and any vulnerabilities that those assets are exposed to.

The potential threats should have already been identified in the SSA (safety mgmt. system Risk Library) and mitigated via the SSP. However, it is necessary to understand the likely impact of these threats to the cyber security of the ship and ship's systems. When considering threat scenarios and types of undesired event, the Company should include incidents from ransomware, to geotagging on social media, to the impact of natural disasters.

The risk assessment should consider the nature of harm that may be caused to the ship, shipboard personnel, passengers, other assets and personnel; and/or the benefits the ship exists to deliver, be they societal, environmental and/or commercial. The cyber security risk will depend on the likelihood that a threat actor can exploit one or more vulnerabilities and cause the nature of harm identified.

An example template for the conduct of a cyber security risk assessment located at 1.4.5

1.4 Risk Assessment

- 1.4.3 Implementation

GUIDANCE
Firstly, the company must carry out context establishment to understand what exactly is in scope for risk assessment, what metrics are used and what governance model is to be in place. The following must be addressed: • What assets on the vessels are to be covered in the cyber risk assessment • Who is doing what? Will vessels have individual risk assessments, or will it be done under a group process (or class) on shore with input from vessels? • Determine the list of identified threats. • Define a list of identified vulnerabilities. • Confirm the process, people, tools and time for conducting the risk assessment.
Once the cyber risk context is established, the company can then analyze the risks by: • Determining if any threats can exploit any vulnerabilities within a nominated asset (see 1.4.5 for an example risk assessment document). • Using a risk scoring matrix, a score can then be allocated to each identified risk. • Risks can be then be put forward for acceptance, avoidance, treatment or transfer (see 1.4.7).
Once a risk has been identified on-board a vessel that requires treatment, a Risk Treatment Plan should be completed, which will look at what controls could be put in place to mitigate the risk ratings (controls to be logical, administrative or physical). The plan should also determine implementation and run and costs, as well as supplemental resources as necessary. These can then be presented to the assigned risk owner for approval and subsequent implementation.
Risks should be monitored at all stages of the risk management process. There should be a process to monitor the effectiveness of controls against risks, to see if any changes to the threats or vulnerabilities require enhancements to the implemented security controls.

1.4 Risk Assessment

- 1.4.4 Documentation

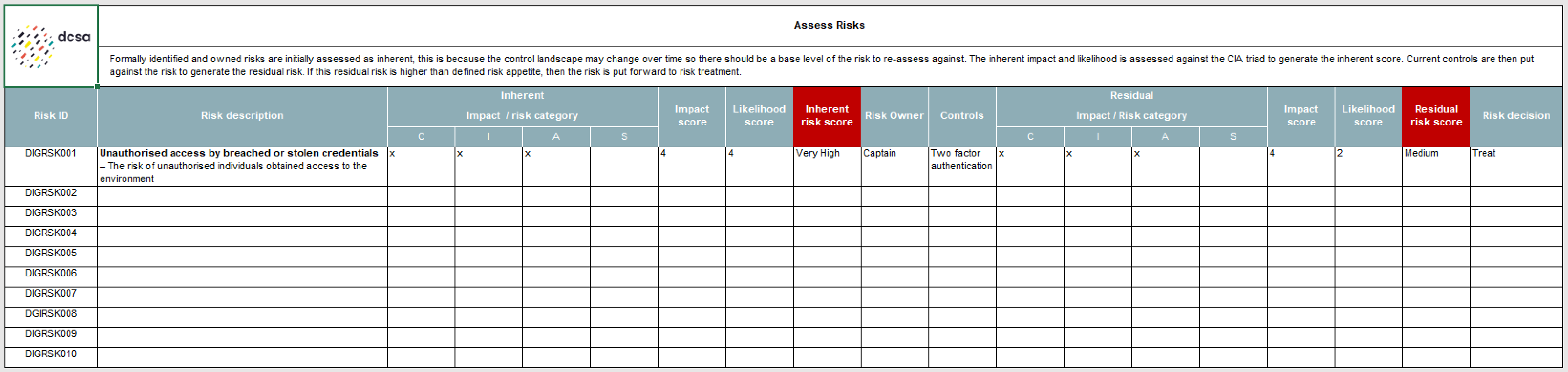
DOCUMENTATION
In order to accurately conduct risk assessments for assets on-board vessels, the following documentation should be produced: a) A company specific guideline document, which can be used to assist staff in conducting risk assessments inline with corporate policies and governance. b) Complete Asset Inventory (1.1) c) Cyber Threat Reporting - to produce a list of cyber threat agents, motivations and objectives. d) A point to note is that not all threats are external so internal threats will also need to be captured, this can come from post incident reporting, anonymous reporting or previous and enterprise level risk assessments. e) Community reporting. f) List of vulnerabilities within assets. This can come from several sources such as vulnerability scanning, vendor information, and risk reporting. g) Impact Assessments for each asset, in order to understand the impact of the loss of that asset (irrespective of the action that causes the loss).

1.4 Risk Assessment

- 1.4.5 Example information security risk assessment

- The table below demonstrates an example Cyber Security Risk Assessment which has been modified for use for IT and OT assets on-board vessels. This should be linked to the asset inventory in 1.1.

- Threats and vulnerabilities against assets will result in a defined risk which is entered here for analysis and risk scoring, to assist in risk evaluation and subsequent risk decision making (Treat, Transfer, Accept or Avoid).



Assess Risks

Formally identified and owned risks are initially assessed as inherent, this is because the control landscape may change over time so there should be a base level of the risk to re-assess against. The inherent impact and likelihood is assessed against the CIA triad to generate the inherent score. Current controls are then put against the risk to generate the residual risk. If this residual risk is higher than defined risk appetite, then the risk is put forward to risk treatment.

Risk ID	Risk description	Inherent Impact / risk category				Impact score	Likelihood score	Inherent risk score	Risk Owner	Controls	Residual Impact / Risk category				Impact score	Likelihood score	Residual risk score	Risk decision
		C	I	A	S						C	I	A	S				
DIGRSK001	**Unauthorised access by breached or stolen credentials** – The risk of unauthorised individuals obtained access to the environment	x	x	x		4	4	Very High	Captain	Two factor authentication	x	x	x		4	2	Medium	Treat
DIGRSK002																		
DIGRSK003																		
DIGRSK004																		
DIGRSK005																		
DIGRSK006																		
DIGRSK007																		
DGIRSK008																		
DIGRSK009																		
DIGRSK010																		

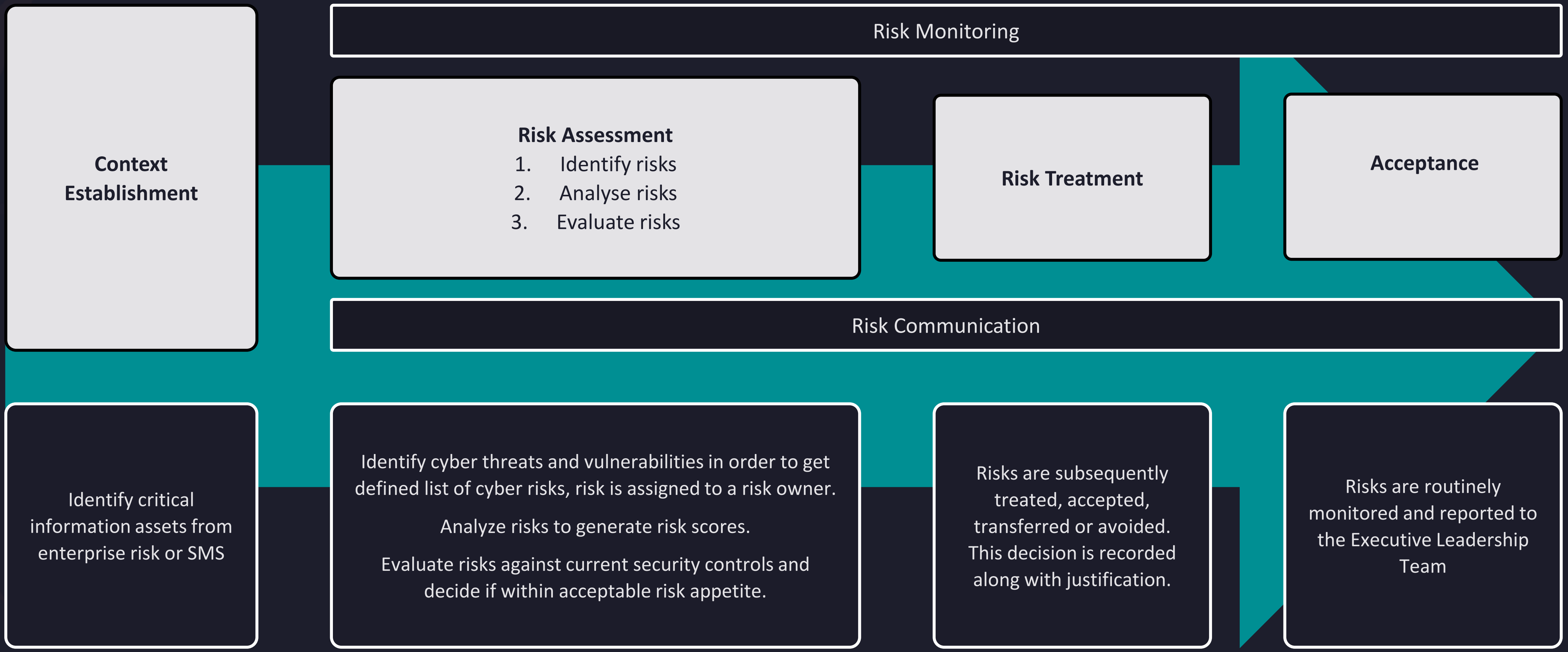
Risk / Impact Category Legend:

C:	Confidentiality
I:	Integrity
A:	Availability
S:	Safety

1.4 Risk Assessment

1.4.6 Process

This page outlines a standard cyber security risk management process, aligned to the NIST Special Publication 800-37.



Risk Monitoring

Context Establishment

Identify critical information assets from enterprise risk or SMS

Risk Assessment

1. Identify risks
2. Analyse risks
3. Evaluate risks

Identify cyber threats and vulnerabilities in order to get defined list of cyber risks, risk is assigned to a risk owner.

Analyze risks to generate risk scores.

Evaluate risks against current security controls and decide if within acceptable risk appetite.

Risk Treatment

Risks are subsequently treated, accepted, transferred or avoided. This decision is recorded along with justification.

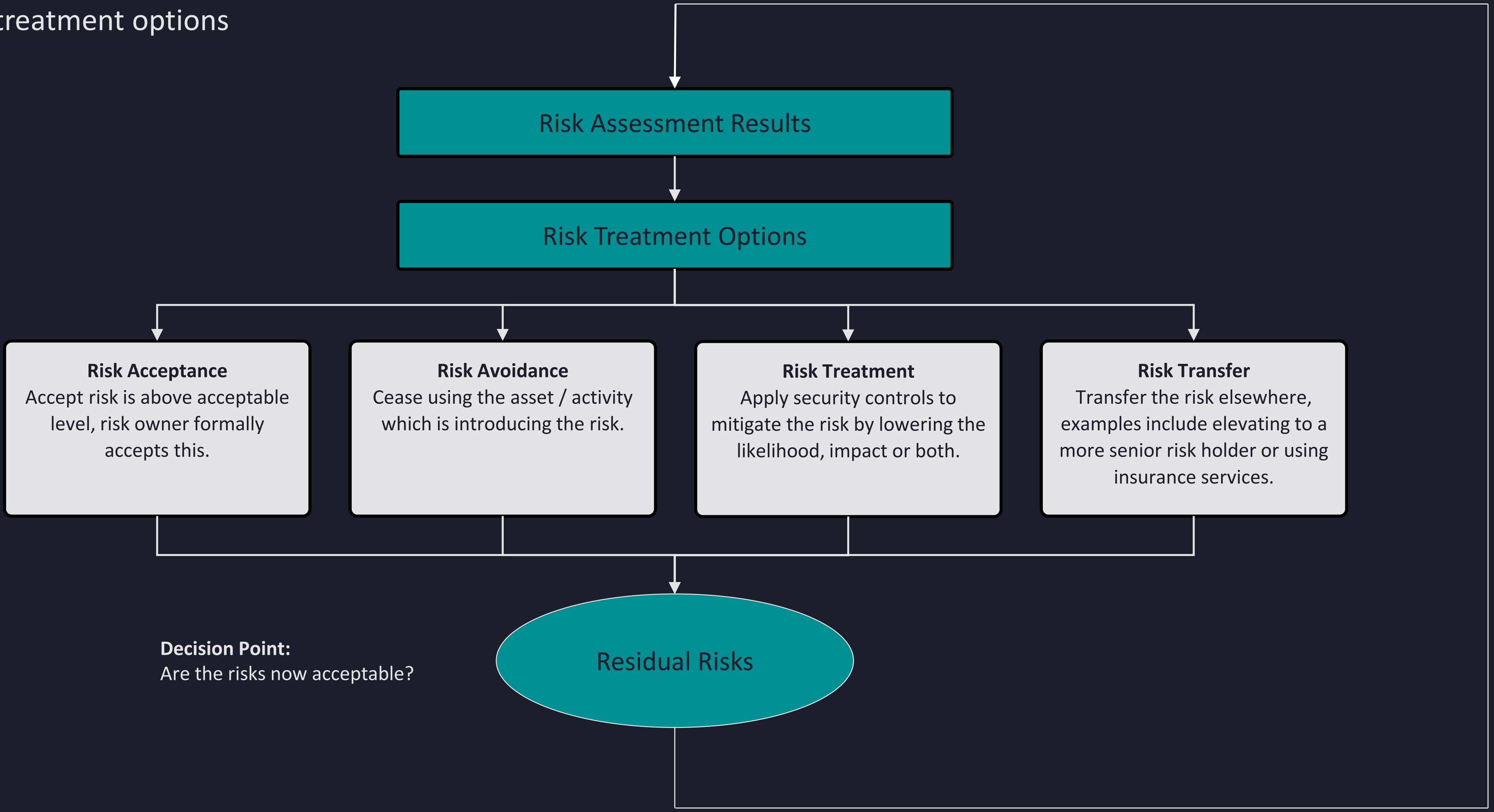
Acceptance

Risks are routinely monitored and reported to the Executive Leadership Team

Risk Communication

1.4 Risk Assessment

1.4.7 Risk treatment options



Risk Assessment Results

Risk Treatment Options

Risk Acceptance
Accept risk is above acceptable level, risk owner formally accepts this.

Risk Avoidance
Cease using the asset / activity which is introducing the risk.

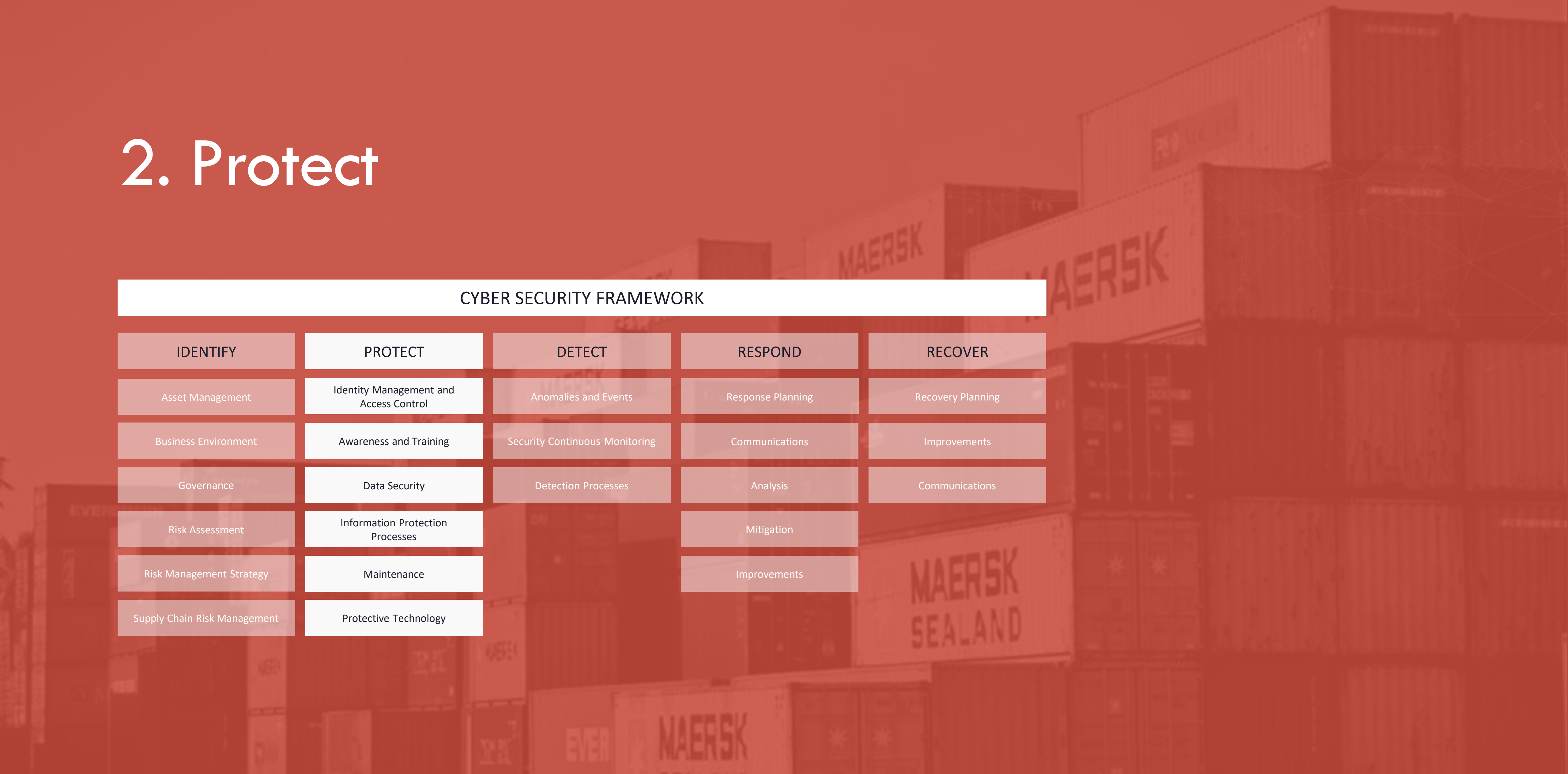
Risk Treatment
Apply security controls to mitigate the risk by lowering the likelihood, impact or both.

Risk Transfer
Transfer the risk elsewhere, examples include elevating to a more senior risk holder or using insurance services.

Residual Risks

Decision Point:
Are the risks now acceptable?

2. Protect



CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

2.1 Identity Management and Access Control

2.1 Identity Management and Access Control

- 2.1.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 11.2 • 11.5	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
	PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, SC-7
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational risks)	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

2.1 Identity Management and Access Control

- 2.1.2 Explanation

EXPLANATION

Identity management and access control, is the process of ensuring that access to information assets is only granted to those who have been approved and can verify that they are who they say they are.

There should be an Access Control Policy place which can be included as part of the overarching Information Security Policy and broken down into multiple policies reflecting the complex nature of a specific organisation. The procedures can be established for the security program in general and for particular information systems as required.

The organisational risk management strategy is a key factor in establishing policy and procedures.

Examples of systems that would require identity management and access controls applied to them on-board vessels could include:

- End user devices, such as company laptops
- Network infrastructure such as wireless access points
- OT systems

2.1 Identity Management and Access Control

- 2.1.3 Implementation

GUIDANCE
Ensure that there is an Access Control Policy in place, which includes all assets that are listed in the Asset Management inventory. Risk management should provide a useful input for the selection and prioritisation of access control requirements.
Ensure that assets on vessel which require identity management and access control have defined access requirements for users / groups. This should be approved by the Asset Owner (listed on the asset management inventory).
Ensure that there is a process for the different approvals (user, admin accounts) as well as other attributes as required.
Ensure that on-vessel assets are part of an identity access and management lifecycle. This will ensure that accounts are authorised, created, monitored and removed as appropriate.
Ensure that there is a role responsible for managing user accounts and passwords on-board. Periodic checks must be held to ensure that there are no default passwords in use and that unused / unrequired user accounts are removed.

2.2 Awareness and Training

2.2 Awareness and Training

- 2.2.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 3 • 5.6	PR.AT-1: All users are informed and trained	AT-2, PM-13
	PR.AT-2: Privileged users understand their roles and responsibilities	AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	PS-7, SA-9, SA-16
	PR.AT-4: Senior executives understand their roles and responsibilities	AT-3, PM-13
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	AT-3, IR-2, PM-13

2.2 Awareness and Training

- 2.2.2 Explanation

EXPLANATION

Humans are invariably the weakest part of any cyber defence profile. Increasingly complex technology means that mistakes can be made. Such as clicking on malicious links in emails, executing malicious files and introducing malware to a system or environment via USB. In addition to this, security short cuts, such as use of weak passwords will often reduce the overall security level of a company.

Companies must therefore determine the appropriate content of security awareness training and security awareness techniques based on the specific organisational requirements and the information systems to which personnel have authorised access. This should take into account factors such as the company's risk appetite, the number of staff, the ability to take on extra training and duties. As well as language and cultural influences.

Within this guideline, the content will specifically be for crew members on-board vessels. The content includes a basic understanding of the need for information security and the user actions necessary to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories / notices from senior company officials, displaying screen messages at logon, and conducting information security awareness events.

2.2 Awareness and Training

- 2.2.3 Implementation

GUIDANCE
There should be a formal process to define the training and awareness requirements for crew members on-board vessels. This should include different phases; such as when an individual is new to a role, after responsibility changes to a role, periodic refreshed training, and corrective training where individuals need to improve. It may be worth conducting audience segmentation, where different groups with different anticipated exposure levels to IT and OT assets have different training and awareness curriculums. An example of this could be: • **Group 1** – Specialists with dedicated information security roles, such as Incident Responders or roles that hold administrator level access. Any seafarer who has designated security duties shall undertake approved security training meeting the requirements of Table A-VI/6-2 of the STCW (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) • **Group 2** – Generalists with user access to critical systems. All seafarers must receive approved security awareness training or instruction that can be conducted on-board ship or ashore. This is not ship-specific and only has to be completed once. • **Group 3** – All other crew. All people employed or engaged on a seagoing ship must receive security-related familiarization training conducted by the Ship Security Officer or other equally qualified person. *STCW alignment is necessary to meet the Designated Cyber Security duties requirement.
Training can be split into two focused areas on-board a vessel. 1 - Awareness and training with regards to how to avoid risks. 2 - Awareness and training of steps to take should a risk become an issue.
General awareness of the types of risks that are posed to a vessel should be communicated to crew members, as well as the preventative steps that can be taken to avoid these risks. This can include basic advice such as recognizing phishing emails or the dangers of using USB drives.
Incident Response training should be provided to an appropriate crew member or members and should align with existing Incident Response plans . For example, crew members may only need to know who to call, or how to recognize an incident on the information system. System Administrators may require additional training on how to respond to and remediate incidents. Incident Responders may receive more specific training on containment, forensics, reporting, system recovery, and restoration. Incident Response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

2.3 Data Security

2.3 Data Security

- 2.3.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 6	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28
	PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16
	PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5
	PR.DS-5: Protections against data leaks are implemented	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7
	PR.DS-7: The development and testing environment(s) are separate from the production environment	CM-2
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	SA-10, SI-7

2.3 Data Security

- 2.3.2 Explanation

EXPLANATION

Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure.

Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, logical controls, organisational standards, and other safeguarding techniques that limit access to unauthorised or malicious users or processes.

Why is Data Security Important?

- All businesses today deal in data. From the banking giants dealing in massive volumes of personal and financial data, to the one-man business storing the contact details of his customers on a mobile phone, data is at play in companies both large and small.

The primary aim of data security is to protect the data that an organisation collects, stores, creates, receives or transmits. Compliance is also a major consideration. It doesn't matter which device, technology or process is used to manage, store or collect data; it must be protected. Data breaches can result in litigation cases and huge fines, not to mention damage to a company's reputation. The importance of shielding data from security threats is more important today than it has ever been as the adversary is becoming increasingly sophisticated in their methods of attack.

2.3 Data Security

- 2.3.3 Implementation

GUIDANCE
Information flow control should be implemented on systems that pose a data security risk. Flow control restrictions include, keeping export-controlled information from being transmitted in the clear over the internet, blocking outside traffic that claims to be from within the organisation, restricting web requests to the internet that are not from the internal web proxy server, and limiting information transfers between organisations based on data structures and content.
Separation of duties addresses the potential for abuse of authorised privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties may have a limited scope on-board vessels, but where there are duties that can be divided amongst a number of roles, this is recommended. As an example this could mean ensuring security personnel administering access control functions do not also administer audit functions.
The principle of least privilege is applied to information system users on-board, meaning that users access information at privilege levels no higher than necessary to accomplish required vessel IT / OT functions.
Configuration baselining should be implemented. Baselined configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baselined configurations serve as a basis for future builds, releases, and/or changes to information systems. Baselined configurations include detail about information system components, network topology, and the logical placement of those components within the system architecture. Maintaining baselined configurations requires creating new baselines as organisational information systems change over time. Baselined configurations of information systems reflect the current vessel architecture.
It is recommended that there is a process to detect unauthorised changes to software and firmware. Any changes must be approved and documented but also any potential impact on security or changes to the risk profile as a result of these actions must be understood, assessed and accepted / treated (if applicable), prior to the change being implemented. Procedures for key on-board operations concerning the safety of the personnel, ship and the protection of the environment should already exist in the SMS. Data security is focused upon the development of instructions determining the actions to be taken if disruption to critical systems is suspected.

2.4 Information Protection Processes and Procedures

2.4 Information Protection Processes and Procedures

- 2.4.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5.7 • 6 • 11	PR.IP-1: A baseline configuration of information technology / industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
	PR.IP-3: Configuration change control processes are in place	CM-3, CM-4, SA-10
	PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9
	PR.IP-5: Policy and regulations regarding the physical operating environment for organisational assets are me	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
	PR.IP-6: Data is destroyed according to policy	MP-6
	PR.IP-7: Protection processes are improved	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
	PR.IP-8: Effectiveness of protection technologies is shared	AC-21, CA-7, SI-4
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
	PR.IP-10: Response and recovery plans are tested	CP-4, IR-3, PM-14
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
	PR.IP-12: A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2

2.4 Information Protection Processes and Procedures

- 2.4.2 Explanation

EXPLANATION
There must be adequate security policies, processes, and procedures which are maintained and used to manage the protection of information systems and assets on-board vessels. Whilst a policy hierarchy potentially detailing processes and procedures may exist within the company already, identifying key processes and procedures on-board vessels in order to ensure the desired levels of confidentiality, integrity, availability and safety is an important part of the cyber security framework. A good example would be to map out the process for dealing with a failure on one of the critical systems on-board the vessel. This can then be drafted as a hard copy guidance document, which would assist a responder in either getting the vessel back to a state of operation without the asset, or the process for restoring the asset back to a working state (either via means of repair or using an alternative asset).

2.4 Information Protection Processes and Procedures

- 2.4.3 Implementation

GUIDANCE
There must be adequate policies in place that protect IT and OT. A specific “Cyber Security on-board Vessels” policy may be an efficient way to address the specific challenges and environment of IT / OT on-board vessels, as well as the unique risks that they face.
The organisation develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing monitoring, assessment and reporting of security events that may pose a risk to the vessel. This can be through activities such as after-action reviews, event log reviews, security assessments and anonymous reporting.
There should be a Change Management Process to ensure that analysis of potential changes to any IT / OT system is conducted to determine potential security impacts prior to change implementation.
Where there is a risk of loss of critical assets, backups should be made that are accessible on-board. System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organisations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organisational requirements for backing up information.
It is important that a vessel develops and implements a Security Incident Response Plan. As part of a comprehensive incident response capability, the vessel should consider the coordination and sharing of information with external organisations. Including, for example, external service providers and organisations involved in the supply chain for organisational information systems. Physical Security is an important aspect of cyber security on-board in terms of restricting access and preventing unauthorised access to critical system network infrastructure on the vessel. The Ship Security Plan (SSP) under International Ship and Port facilities Security (ISPS) code addresses the specific identification of restricted areas and preventive action against access to any such designated areas. Measures should be taken to restrict access to critical systems and network infrastructure. In addition the SSP should have a reference to the cyber risk management chapter in SMS.

2.5 Maintenance

2.5 Maintenance

- 2.5.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 11.1	PR.MA-1: Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools	MA-2, MA-3, MA-5, MA-6
	PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access	MA-4

2.5 Maintenance

- 2.5.2 Explanation

EXPLANATION
Software maintenance is to be included as part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. It is recommended that maintenance and patching cycles occur on a cycle no greater than once a month. As with conventional system maintenance, any asset (software or hardware) that undergoes some form of maintenance such as patching, updating or hardening may introduce new risks onto the vessel if not applied correctly. Therefore it is important that such maintenance is carried out by suitably trained personnel.

2.5 Maintenance

- 2.5.3 Implementation

GUIDANCE

Maintenance activities and processes for IT and OT on-board vessels should include a process that:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and / or organisational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or moved to another location;

c. Requires that there is a process which explicitly approves the removal of the information system or system components from organisational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organisational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes updates to organisational maintenance records.

Maintenance activities involving any IT or OT assets should also be verified and authorised by a role such as the CySO to ensure that activities such as patching, updating, hardening or modification of both IT and OT software, hardware or firmware does not introduce any cyber security or safety risks.

2.6 Protective Technology

2.6 Protective Technology

- 2.6.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5.3.4 • 5.4 • 11 • 11.3	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU Family
	PR.PT-2: Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3, CM-7
	PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

2.6 Protective Technology

- 2.6.2 Explanation

EXPLANATION

Protective technology is the use of technology to mitigate risks through several different processes:

Firstly, it is important to understand that the more IT, OT, applications and users you have increases the attack surface of the vessel. Whilst asset management seeks to accurately record and map out what the constituent parts of that attack surface could be, protective technology looks to reduce that attack surface by removing any unnecessary parts of it.

The second area to focus on is the on-board / shore-based communications interface. Assets that have external communication links pose a risk to the vessel.

• **Focus on Communications and Control.**
At the technical level, companies should consider restricting external connections and interfaces to, from, and between specific machines; disabling wireless access; preventing the remote execution of privileged commands; continuously monitoring endpoints to detect, and respond to, indicators of attack; identifying and preventing the transfer of sensitive information through sophisticated data loss prevention and protection solutions; and establishing alternate telecommunications channels for business continuity.

• **Leverage Big Data.**
There seemingly is no end to the amount of event logs that now can be captured, stored, analyzed, correlated, shared and turned into action when next-generation cloud technologies are combined with user-defined response rules. This allows staff to focus more time on governance, risk and compliance, and less time on traditional forensic and audit activities.

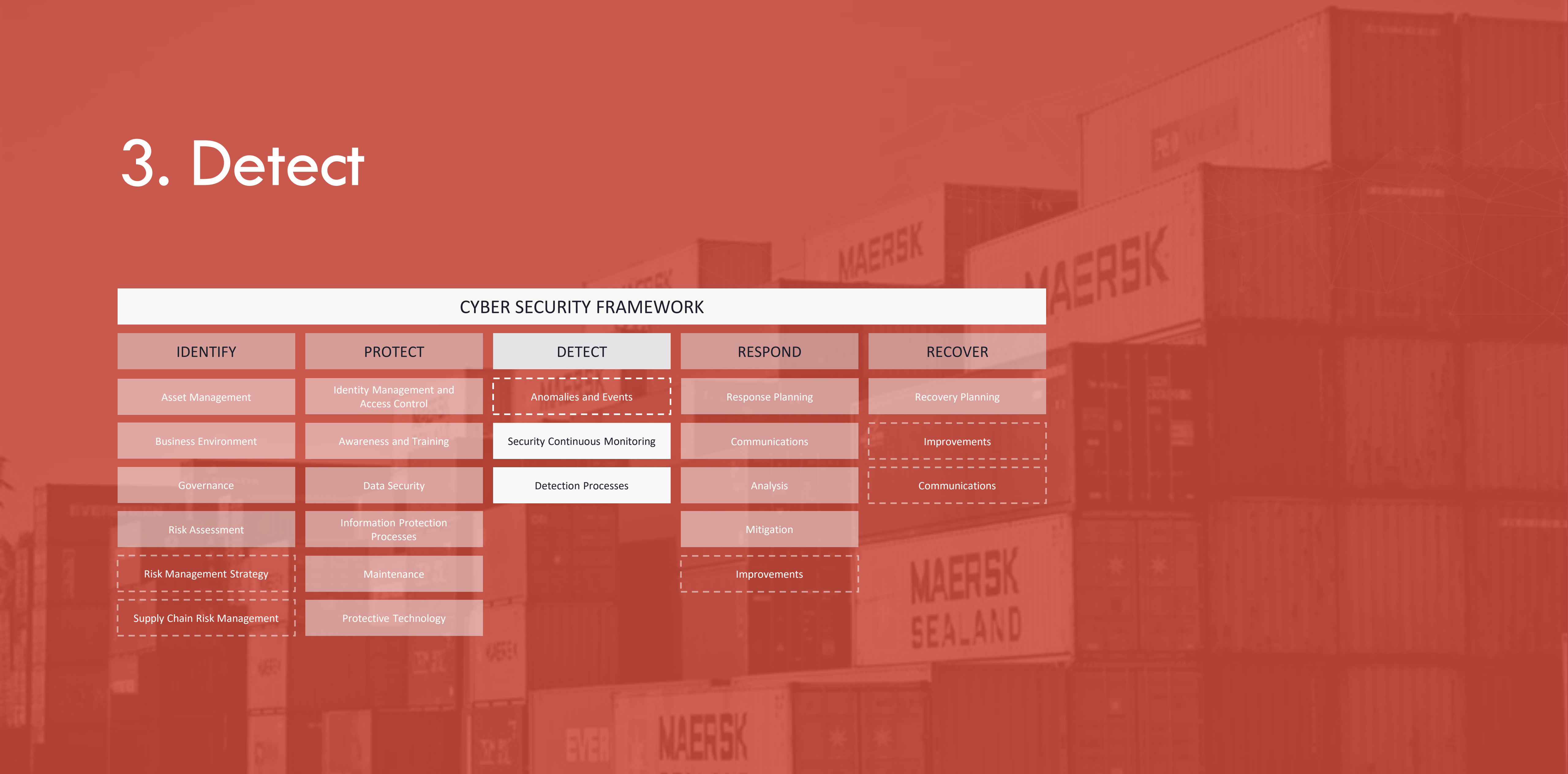
• **Constrain Removable Media.**
External devices pose unique challenges, but technologies exist that can be used to log their use, control access to the data stored on them, and enforce encryption requirements. On the network side, administrators can disable autorun and autoplay options, and block USB ports from working altogether.

2.6 Protective Technology

- 2.6.3 Implementation

GUIDANCE
Detective controls are one way to protect assets on-board systems, using audits and logs to determine the actions surrounding an incident. Knowing that detective controls are in place can also assist in deterring malicious users from carrying out actions that may compromise critical assets.
Removable media poses two distinct risks to vessels. Firstly, removable media can provide an ingress route for malware and secondly it can provide an exfiltration route for protected or sensitive data. Carriers should determine the level of risk they wish to accept with regards to removable media on-board vessels and implement a policy and supporting controls to mitigate unwanted risks. Which could include disabling USB ports, or using “sheep-dips” and sandboxes to test removable media prior to using it on-board a vessel.
Systems that are running unnecessary capabilities or having unnecessary hardware on-board a vessel, introduce a larger attack surface to the vessel as well as a larger burden of system hardening, patching and vulnerability management. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. This should also focus on areas such as disabling unused network ports, functions and protocols within systems.
Technology is leveraged where applicable to ensure that there are protective measures in place to achieve an acceptable level of resilience. This can include failsafe systems, load balancing and backup systems.

3. Detect



CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

3.2 Security and Continuous Monitoring

3.2 Security and Continuous Monitoring

- 3.2.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5.5 • 5.5.1 • 5.5.2 • 11.4	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Malicious code is detected	SI-3, SI-8
	DE.CM-5: Unauthorised mobile code is detected	SC-18, SI-4, SC-44
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4
	DE.CM-7: Monitoring for unauthorised personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Vulnerability scans are performed	RA-5

3.2 Security and Continuous Monitoring

- 3.2.2 Explanation

EXPLANATION

There is a misconception that a cyber security threat will be a visual incident. If you ask someone what an incident looks like they will probably describe systems going offline or alarming ‘random’ images popping up on digital systems. However, this is not accurate and often, it is not visually apparent that a cyber attack has occurred. Sometimes you may sense a problem, but all the digital systems may still seem to agree with each other.

Cyber attacks are not always carried out remotely. A motivated individual, or complicit member of the crew may board the ship and install a compromised device or piece of malware onto the network. Alternatively, crew members may unintentionally introduce malware or other cyber risks to the vessel due to a lack of training, through poor processes or as a result of limited risk awareness.

Once in place, an attacker would have continuous remote access to the on-board network, bypassing the security of all network perimeter defences, such as firewall. Ensuring that cyber security procedures are followed and reminding all personnel to be vigilant will lessen the likelihood of this occurring. The use of monitoring and reporting systems will help identify ongoing threats.

On the occasion that a risk realizes, resulting in a security incident, dealing with both the cause and the effects are critical. Minimising the time between the risk occurring and concluding an incident response process is highly important. In order to limit this response time, an effective detection process should be in place.

For clarity, a **security event** is any observable occurrence that is relevant to cyber security on-board a vessel. This can include attempted attacks or lapses that expose security vulnerabilities**.** A **security incident** is a security event that results in damage or risk to information security assets and operations and must be detected as early as possible.

Security and continuous monitoring can take the form of a number different capabilities such as monitoring event logs from critical assets and network devices using a Security Information and Event Management (SIEM) platform tuned to trigger alerts in the event of insecure or malicious activity on systems. Another option is to periodically review settings and configurations of assets to ensure that they are in the correct state and that there haven’t been malicious or accidental changes.

3.2 Security and Continuous Monitoring

- 3.2.3 Implementation

GUIDANCE
The organisational IT department may invest in specific threat detection systems and / or additional functionality in the ship security suite that can alert personnel to a cyber incident. This may also include the use of Intrusion Detection Systems to detect and alarm on network and host intrusion incidents. Or deployment of security information event management solutions to accumulate event logs, perform correlation and alarm on discovered malicious activity. Threat detection systems such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) should be included in the Asset Register.
The organisation should employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process. Organisations should determine the required vulnerability scanning frequency for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.
Other methods of detecting a cyber incident include, which may or may not be covered by a threat detection system: • Noting unusual password activity. For example, where a department account or crew member account is locked out and a request is made to change the password. Especially if the user did not initiate the action. • Being aware that the sudden appearance of suspicious pop-ups and other adware, especially when browsing the internet, usually indicates unsafe internet browsing • Investigating when computers, the network and other services may be slower than normal or unresponsive to the user. If a slower than expected seed occurs, this should be investigated further (for example, by conducting a virus scan) and reported to the IT department. • Responding to the confirmation of a breach. For example, where a computer is locked out and a ransom payment is demanded, or where a key logger / physical device of unknown origin is found connected to an end user device such as a laptop. If ransomware suddenly appears, the first actions should always be to quickly disconnect the computer from the network. This also applies to all cases where a virus / infection is suspected. The infected device should only be reconnected following confirmation from the IT department.

3.3 Detection Processes

3.3 Detection Processes

- 3.3.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 8	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	CA-2, CA-7, PM-14
	DE.DP-2: Detection activities comply with all applicable requirements	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
	DE.DP-3: Detection processes are tested	CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
	DE.DP-4: Event detection information is communicated	AU-6, CA-2, CA-7, RA-5, SI-4
	DE.DP-5: Detection processes are continuously improved	NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

3.3 Detection Processes

- 3.3.2 Explanation

EXPLANATION

There are several ways of detecting if a security event or incident is in progress. Sometimes these will be simple to identify as a system may stop working, display erroneous results, slow down or lock a user out. However, other incidents which can carry more risk are when the incident has not been detected, this is particularly true for systems that require high levels of integrity, such as the vessel's ECDIS system.

In order to ensure that systems have an adequate level of availability, data maintains integrity and accuracy, it is important to have a robust detection process in place. The level of detection will depend on individual carriers' risk appetite and technological dependencies but may include some of the following options:

- Security Information & Event Monitoring (SIEM). Hardware / software that aggregates event logs and flows from network architecture, applications, end user devices, firewalls, and other devices, in order to alert security staff to anomalous events and indicators of compromise which could signal a security incident.
- Manual review. For organisations with lower demands of security detection, manual review of logs, whilst time consuming can give an indication of patterns of events that could indicate a security incident.
- Vulnerability scanning. Over time, assets may increase the number of vulnerabilities they have as attackers develop new techniques and new exploits are found. Frequent vulnerability scanning will allow carriers to identify weaknesses to be remediated by security staff, as well as an opportunity to patch or update the asset.

3.3 Detection Processes

- 3.3.3 Implementation

GUIDANCE
Confirm that the SMS addresses procedures relating to detecting and reporting cyber incidents and the prevention of non-conformities with organizational security policies. When incorporating Cyber Risk Management (CRM) into the SMS, company reporting requirements for incidents may need to be updated to include cyber related incidents. Examples of such incidents and cyber incidents could be as follows: • Unauthorised access to network infrastructure • Unauthorised or inappropriate use of administrator privileges • Suspicious network activity • Unauthorised access to critical systems • Unauthorised use of removable media • Failure to comply with software maintenance procedures • Failure to apply malware and network protection updates • Loss or disruption to the availability of critical systems • Loss or disruption to the availability of data required by critical systems. Corrective and preventive measures should be documented after conducting root-cause analysis.
Vessels should be included in the development and maintenance of a continuous monitoring strategy and implement a continuous monitoring program that includes: • Establishment of metrics to be monitored and the frequency for monitoring • Ongoing security control assessments in accordance with the organisational continuous monitoring strategy; • Ongoing security status monitoring of organisation-defined metrics in accordance with the continuous monitoring strategy; • Correlation and analysis of security related information generated by assessments and monitoring; • Response actions to address results of the analysis of security-related information; and The above should be included in the Safety Management Review conducted regularly as per the ISM code.
The organisation implements a process for ensuring that organisational plans for monitoring activities associated with organisational information systems are developed, maintained and executed in a timely manner. This may include determining the risks posed by organisational systems and including security requirements within them such as potential log sources for monitoring as part of a security information and event monitoring capability.

4. Respond

CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

4.1 Response Planning

4.1 Response Planning

- 4.1.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 7 • 9.2 • 9.3	RS.RP-1: Response plan is executed during or after an incident	CP-2, CP-10, IR-4, IR-8

4.1 Response Planning

- 4.1.2 Explanation

EXPLANATION

A Security Incident Response plan ensures that each cyber incident is reported, investigated, contained and remediated. In the event of a security incident it is vital, from both a business and a safety perspective, that a ship is able to operate without disruption or compromise of on-board essential systems.

A vessel should therefore have in place a Security Incident Management Plan which is based upon:

- Procedures for both incident response plans and preparation
- A process that initiates on the detection of an incident
- Clear communications guidelines for crew, covering reporting lines on-board the vessel and back to company headquarters ashore.
- A process to record incident response steps and activities
- A process for handling forensic evidence is in place

Incident response on-board vessels provides a unique challenge to crew members, the following should be taken into account:

- Any additional incident response capability on-board a vessel will require crew member competencies that sit outside of standard IT operations.
- It is recommended that there is a role on each vessel formally appointed as the point of contact for cyber security incidents on that vessel.

It will also be necessary for consideration to be given to when and how forensic evidence will be preserved to aid in any investigation into the cause of the event or the perpetrators. Where evidence collection is for law enforcement purposes it should be in accordance with the relevant national guidelines.

In the event of an incident involving the loss or theft of ship data, unauthorised access to ship data or systems, or interference with computer systems, the CSO or CySO should notify the relevant parties and law enforcement agencies. When Personally Identifiable Information (PII) is lost, stolen or compromised, the CSO or CySO should ensure that the relevant Information Commissioner or Data Protection Authority and impacted individuals are notified.

The CSO or CySO should ensure that discovery procedures are established in all appointment documents and contracts, including, where applicable, in non-disclosure agreements. Following any security breach or incident, an important post-incident activity is the formal evaluation of the way that the event was handled, to determine lessons that can be learned and to review whether any changes are required to the security assessments, security plans or supporting policies, processes and procedures.

4.1 Response Planning

- 4.1.3 Implementation

GUIDANCE

The following elements should be considered when drafting incident response planning:

(a) Information on cyber security responsibilities and links to organisations that will assist the ship in the event of a cyber security incident, such as a dedicated incident response team, Security Operations Center or forensic capability.
(b) The cyber security drills to be practiced to test the ship's and shipboard personnel's response to cyber security incidents.
(c) The cyber security of communications, including those:

- Between personnel with security responsibilities;
- Between those responsible for technical security and the wider security team; and
- Providing information about the ship and ship assets to third parties.

Existing Emergency / Incident Response Plans should be updated to include Security Incident response procedures and associated Communications Plans. A cyber risk management competent resource must be added to the emergency response team already established in the SMS.

The Security Incident Response plan should be created for the purpose of addressing security events and incidents and should enable an effective and coordinated response. This will require an assessment of potential risks to the ship, its function, ship assets, and the role of personnel and third parties in the event of a security breach or incident. This section should include:

a. Risk mitigation measures including: the forensic readiness measures required to enable the capture of forensic information about an incident for use by law enforcement, and / or detailed analysis of the root causes of the incident;
   - The process to be followed on discovery of a breach / incident (including near misses, i.e. narrow avoidance of a security breach / incident);
   - Business continuity measures required in the event of ship system failure, impairment or non-availability;
   - The disaster / incident recovery actions required in the event of serious failure scenarios; and
   - Steps to be taken to contain and recover from the event.

b. The review process to be followed after a security breach or incident, including both assessment of any on-going risk and evaluation of the response to the breach or incident by the SSO and where appropriate the supply chain.

c. The need for contractual provisions to handle breaches / incidents caused by a third party connected to the ship. For example, a professional advisor, contractor or supplier.

d. The arrangements for shipboard personnel to implement in conjunction with existing business continuity planning and exercises.

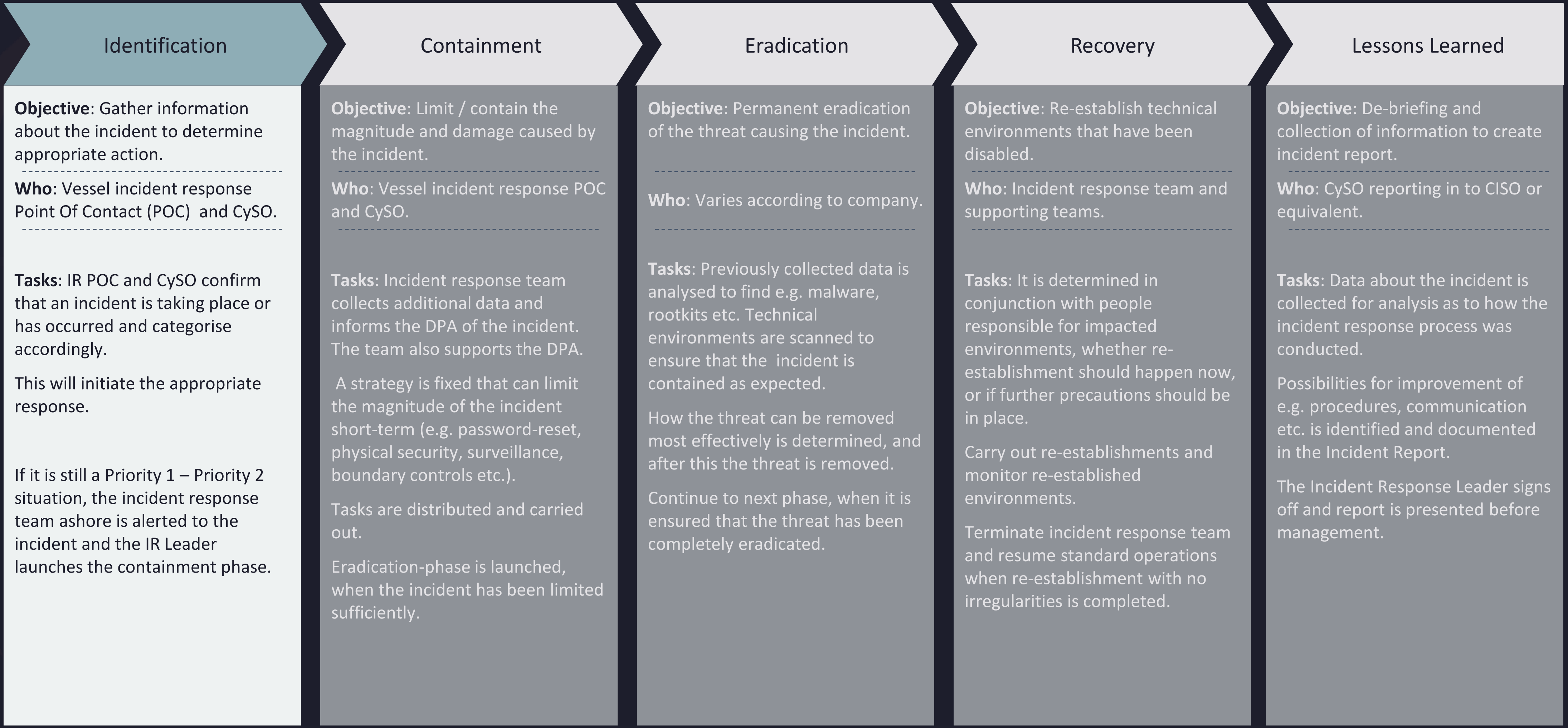
4.1 Response Planning

- 4.1.4 Top recommendations for incident response on-board vessels

RECOMMENDATIONS
Introduce a Situation Assessment Process. The SBAR (Situation, Background, Assessment, and Recommendation) handoff protocol used in Emergency Medical Service teams is a clear and rapid way to appraise and communicate a situation where there may be a lack of clarity and a sense of urgency/safety. It promotes clear and accurate communication among team members while simultaneously creating a more cohesive shared mental model about what pieces of information are important or necessary to share in verbal and written communication. An SBAR playbook to be held on vessels and practised with is recommended.
Use checklists. When a cyber incident occurs, it is a natural response that individuals / teams will act in what they deem to be the best manner. This can be based on situational awareness, department priorities, or a fear of inaction. In order to ensure that all logical steps are followed, a checklist (or incident specific checklists) can be created, practised and used in order to ensure a logical and sequential response. Keeping a “hard copy” of checklists as opposed to storing them on an IT system is also recommended in case the asset that they are stored on is affected by the cyber incident.
Maximize cross-training. With two distinct teams that may be involved in responding to a cyber incident on-board a vessel (on-vessel and on-shore), cross training is an essential ongoing requirement. Cross training should: • Ensure that every role holder understands their role in the incident response process • Promote an understanding of supporting roles within the incident response capability • Clarify and practise communication protocols (also consider if primary communication systems are affected by an attack, is everyone aware of a secondary means of communications and how to use them?)

4.1 Response Planning

4.1.5 Example of an incident response process with example phases



Identification

Objective: Gather information about the incident to determine appropriate action.

Who: Vessel incident response Point Of Contact (POC) and CySO.

Tasks: IR POC and CySO confirm that an incident is taking place or has occurred and categorise accordingly.

This will initiate the appropriate response.

If it is still a Priority 1 – Priority 2 situation, the incident response team ashore is alerted to the incident and the IR Leader launches the containment phase.

Containment

Objective: Limit / contain the magnitude and damage caused by the incident.

Who: Vessel incident response POC and CySO.

Tasks: Incident response team collects additional data and informs the DPA of the incident. The team also supports the DPA.

A strategy is fixed that can limit the magnitude of the incident short-term (e.g. password-reset, physical security, surveillance, boundary controls etc.).

Tasks are distributed and carried out.

Eradication-phase is launched, when the incident has been limited sufficiently.

Eradication

Objective: Permanent eradication of the threat causing the incident.

Who: Varies according to company.

Tasks: Previously collected data is analysed to find e.g. malware, rootkits etc. Technical environments are scanned to ensure that the incident is contained as expected.

How the threat can be removed most effectively is determined, and after this the threat is removed.

Continue to next phase, when it is ensured that the threat has been completely eradicated.

Recovery

Objective: Re-establish technical environments that have been disabled.

Who: Incident response team and supporting teams.

Tasks: It is determined in conjunction with people responsible for impacted environments, whether re-establishment should happen now, or if further precautions should be in place.

Carry out re-establishments and monitor re-established environments.

Terminate incident response team and resume standard operations when re-establishment with no irregularities is completed.

Lessons Learned

Objective: De-briefing and collection of information to create incident report.

Who: CySO reporting in to CISO or equivalent.

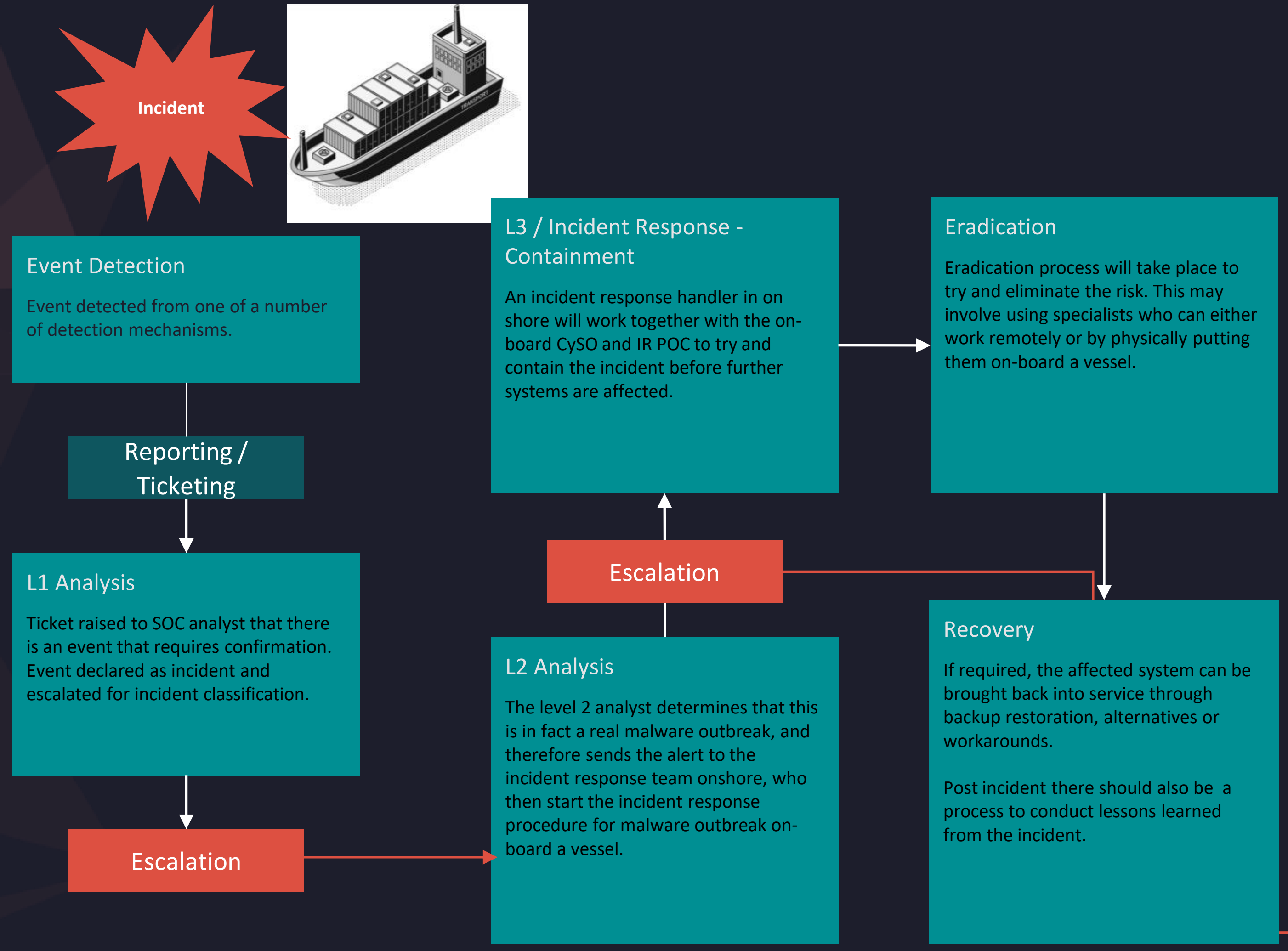
Tasks: Data about the incident is collected for analysis as to how the incident response process was conducted.

Possibilities for improvement of e.g. procedures, communication etc. is identified and documented in the Incident Report.

The Incident Response Leader signs off and report is presented before management.

4.1 Response Planning

4.1.6 Example incident response process linking incident escalation to an example impact level table*



Event Detection

Event detected from one of a number of detection mechanisms.

Reporting / Ticketing

L1 Analysis

Ticket raised to SOC analyst that there is an event that requires confirmation. Event declared as incident and escalated for incident classification.

Escalation

L2 Analysis

The level 2 analyst determines that this is in fact a real malware outbreak, and therefore sends the alert to the incident response team onshore, who then start the incident response procedure for malware outbreak on-board a vessel.

Escalation

L3 / Incident Response - Containment

An incident response handler in on shore will work together with the on-board CySO and IR POC to try and contain the incident before further systems are affected.

Eradication

Eradication process will take place to try and eliminate the risk. This may involve using specialists who can either work remotely or by physically putting them on-board a vessel.

Recovery

If required, the affected system can be brought back into service through backup restoration, alternatives or workarounds.

Post incident there should also be a process to conduct lessons learned from the incident.

Potential Impact	Definition	In Practice
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organisational assets, or individuals.	A limited adverse effect means that a security breach might: (i) cause a degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organisational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, assets or individuals.	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, assets, environment or individuals.	A severe or catastrophic adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organisation is not able to perform one or more of its primary functions; (ii) result in major damage to environment and/or organisational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

*Aligned to "The Guidelines on Cyber Security on-board Ships", Version 3.

4.2 Communication

4.2 Communication

- 4.2.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 9.3	RS.CO-1: Personnel know their roles and order of operations when a response is needed	CP-2, CP-3, IR-3, IR-8
	RS.CO-2: Incidents are reported consistent with established criteria	AU-6, IR-6, IR-8
	RS.CO-3: Information is shared consistent with response plans	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	CP-2, IR-4, IR-8
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SI-5, PM-15

4.2 Communication

- 4.2.2 Explanation

EXPLANATION

Communication is an essential part of preparing for, implementing and operating a cyber-secure vessel. Cyber security related communication can be broken down in two distinct areas on-board vessels:

a) Preparatory communications. Communicating roles and responsibilities, new processes, governance.
b) Incident response communications. Once an incident has occurred, the process(es) for communicating the incident, its effect on the vessel, potential actions crew should take and communication with shore-based specialists and stake holders.

4.2 Communication

- 4.2.3 Implementation

GUIDANCE
The recommended content of a Communication Plan should include as a minimum: (a) Information on cyber security responsibilities and links to organisations that will assist the ship in the event of a cyber security incident (b) Communication timescales (c) Alternative methods of communication (d) The cyber security drills to be practiced to test the ships and shipboard personnel’s ability to manage cyber security incidents. - The requirement for Ship-shore emergency drills with the participation of the head-office is related to safety (ISM) and security (ISPS). - For the time being Security drills include “Piracy” , “Bomb Threat” , “Stowaways on-board”. “Cyber Security attack” should be included as a possible scenario. (a) The cyber communications, including those: - Between personnel with security responsibilities - Between those responsible for technical security and the wider security team; and - Providing information about the ship and ship assets to third parties

4.3 Analysis

4.3 Analysis

- 4.3.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 9.4	RS.AN-1: Notifications from detection systems are investigated	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	RS.AN-2: The impact of the incident is understood	CP-2, IR-4
	RS.AN-3: Forensics are performed	AU-7, IR-4
	RS.AN-4: Incidents are categorized consistent with response plans	CP-2, IR-4, IR-5, IR-8
	RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SI-5, PM-15

4.3 Analysis

- 4.3.2 Explanation

EXPLANATION

The ISM Code recognizes that incidents generally fall into two categories:

(a) Those considered to be sufficiently serious that they should be reported to the relevant authorities by the CSO, for example:

- Unauthorised access to, misuse or fraudulent use of sensitive ship systems;
- Unauthorised changes to or loss of information from sensitive ship systems;
- Attempted or successful cyber-attacks on ship systems affecting the safety of life, the ship or its cargo;
- Damage to the ship, where it is suspected or evident that a cyber security breach or breaches are a contributory factor;
- Attempts to manipulate cargo manifests to facilitate the smuggling, illegal or unauthorised carriage of prohibited or controlled goods or materials (for example, illegal drugs, weapons, explosives, items whose carriage is restricted by international treaty, etc.);
- Attempts to affect passengers, for example fraud associated with theft or unauthorised access to personal data or personally identifiable information or compromise of ship systems processing bank or credit card information.

(b) Those of a less serious nature, but which require reporting to, and investigation by, the SSO and for cyber incidents the CySO, for example:

- Cyber security incidents affecting the ship and/or its cargo that are not covered by the examples in point (a) (i) above; and
- Malware incidents affecting non-sensitive systems including the personal devices owned by the crew. A cyber security incident is likely to arise from unauthorised access to, misuse or fraudulent use of, ship systems or related assets and may result in:
    1. Loss or theft of assets, including documents and storage media;
    2. Unauthorised access to data or information
    3. Loss, compromise, unauthorised manipulation or change of data or information;
    4. Loss or compromise of ship assets connected to its systems;
    5. Planting of bugs or other surveillance devices; and
    6. Insertion of malicious software.

4.3 Analysis

- 4.3.3 Implementation

GUIDANCE
The organisation develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of organisation defined metrics to be monitored; b. Establishment of organisation defined frequencies for monitoring, and organisation defined frequencies for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organisation continuous monitoring strategy; d. Ongoing security status monitoring of organisation defined metrics in accordance with the organisation continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; g. Reporting the security status of the organisation and the information systems to organisation defined personnel or roles in line with the organisation defined reporting frequency
The organisation: a. Reviews and analyses information system audit records in line with the frequency defined by the organisation for indications of organisation defined forms of inappropriate or unusual activity; b. Reports findings to the responsible personnel or roles, as determined by the organisation. c. Internal audits carried out by head-office representatives on-board for safety and security should include cyber security related forms, procedures and plans.

4.4 Mitigations

4.4 Mitigation

- 4.4.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 10	RS.MI-1: Incidents are contained	IR-4
	RS.MI-2: Incidents are mitigated	IR-4
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	CA-7, RA-3, RA-5

4.4 Mitigation

- 4.4.2 Explanation

EXPLANATION

This section provides guidance for the identification of mitigation measures to be applied to the people, physical, process and technological aspects of a ship with regards to mitigating cyber security risks.

Whilst there should also be a focus on mitigating any findings that could lead to a non-conformity being declared on-board a vessel, it is envisaged that through early identification of cyber security risks and pre-emptive mitigation activities, these can be avoided.

When choosing mitigation measures, a balance will need to be struck on a case-by-case basis to ensure that:

a) Mitigations do not create other unforeseen risks

b) Mitigations do not have an adverse effect on operations by constraining staff, operational process or severely restricting technological benefits

c) Mitigations are not so disruptive that they are ignored or ”worked around”

Mitigations should be captured in some form of documentation so that they can be monitored for effectiveness, used in the risk management process and updated as required.

Mitigations can also be generated as part of risk treatment in the cyber risk management process.

4.4 Mitigation

- 4.4.3 Implementation - People

GUIDANCE

People are often the weakest element in any secure system or operation, so the interaction of people with the ship systems needs to be understood. It is therefore advised that the answers to the following questions are established as the first stage in the process of deciding upon the mitigation measures which are appropriate and proportionate:

(a) Who needs access to the ship data and systems?
(b) What types of access are required?
(c) How is this access provided, and is it required remotely from the ship?
(d) What access controls will be required (for example, can an individual create, read, update or delete the ship data, and what level of control does an individual have)?
(e) What level of cyber security awareness and understanding of cyber security is required by individuals?
(f) Are contractors, temporary and agency staff provided with cyber security awareness training as part of their induction?
(g) Do individuals understand the ship operator's policies, processes and procedures for the creation, use and maintenance of ship data and the operation and maintenance of vessel systems?
(h) Are processes and procedures in place to update individuals about any changes in policies, processes and procedures?
(i) Are individuals briefed in a timely manner on changes in threats, risks and the required security controls?

The answers to the first four questions will also enable the SSO to identify high-risk positions. The individuals holding those positions should be subjected to appropriate pre-employment / pre-contract security screening and vetting checks, with appropriate on-going monitoring.

High risk positions will include those with:

(a) IT and/or operational system administration responsibilities;
(b) Security roles;
(c) Information Management roles;
(d) Purchasing, finance and contract management roles;
(e) Personnel managers (regarding handling of security breach related disciplinary matters and management of the insider threat).

4.4 Mitigation

- 4.4.3 Implementation - Physical

GUIDANCE

In order to enhance the achievable level of cyber security, it is necessary to have in place physical security measures that:

(a) Prevents unauthorised access to sensitive ship systems, for example:

- IT equipment accessing, processing or storing sensitive information;
- Systems fulfilling safety critical functions; and
- Security and control systems.

(b) Prevents theft of, or damage to:

- IT equipment, storage media, cables, etc.; and
- Ship data, in particular that pertaining to the safe and secure operation of the ship.

(c) Protect network and communications infrastructure from:

- Accidental damage;
- Deliberate / malicious damage; and
- Tampering and / or denial of service.

(d) Protect utilities, heating, ventilation and cooling systems required to:

- Operate the sensitive ship systems;
- Operate the network and communications infrastructure;
- Maintain a safe and secure working environment.

Some ship systems may need to be accorded the same level of physical protection as key operational spaces, with security perimeters defined and implemented to protect not only the systems but also their cabling and any associated power, plant and machinery. It will therefore first be necessary to establish:

(a) What physical and electronic infrastructure is used to create, access, process and store ship data, including any communications and networking components;
(b) The infrastructure that is critical to ensure the ongoing operation of ship systems and any processes or services they support;
(c) The dependencies that parts of the infrastructure have on other critical services or infrastructure;
(d) The extent to which this infrastructure is dedicated to ship systems or shared with different activities;
(e) The extent to which this infrastructure is shared with third parties;
(f) Availability of personnel and external agencies for reaction and response and their ability to access the functional areas.

This information should then be used to decide where physical protective measures are required. Where it is decided that secure perimeters are needed, these should be designed to prevent unauthorised access or tampering and, depending on the location and criticality, may need to be alarmed and monitored by CCTV systems. When considering the level and type of protection to be provided, a defence in depth approach is more reliable than a single protective barrier.

4.4 Mitigation

- 4.4.3 Implementation - Process

GUIDANCE

The failure to develop and maintain appropriate policies and their supporting processes that reflect the operating culture of an organisation can result in them being ignored, or lead to the adoption of informal local practices, resulting in the security or operation of the ship assets being undermined. It is therefore important that processes specific to cyber security are in place which, as a minimum, detail:

(a) The use of externally hosted systems or business portals employing web-based interfaces;
(b) Communications and networking links, whether from externally hosted systems or services, or those hosted at a port or port facility that the ships is visiting;
(c) Wireless networking and communications technologies, for example Bluetooth and Wi-Fi;
(d) Configuration of protective software, such as firewalls, anti-malware products and intrusion prevention / detection applications;
(e) The connection of new computers, mobile devices or IT-controlled operational equipment to the ship's IT infrastructure;
(f) The use of Personal Mobile Radios (PMR) aboard the ship;
(g) Configuration and management of user and systems account privileges, including those of third-party personnel, with access to ship systems. Particularly those controlling power, heating, ventilation and cooling systems for accommodation containing on-site IT systems, or ship security systems. For example: access control, security barrier control, CCTV, etc.;
(h) Connection of personal IT devices or removable media to ship systems;
(i) Access to emails, instant messaging services, external websites or file sharing services from workstations on operational systems (control systems, security systems, etc.);
(j) Mobile time-critical access to data during an emergency. It will also be necessary to have processes in place for:

- Regularly reviewing access privileges to ensure that individuals' privileges are consistent with their job roles and functions; and
- Regularly reviewing systems logs and the investigation of anomalies.

4.4 Mitigation

- 4.4.3 Implementation – Technology I

GUIDANCE

In deciding upon technical mitigation measures that are needed to address cyber security risks, it will first be necessary to gain an understanding of:

(a) The systems in use;
(b) The channels used by systems, sensors and actuators to communicate;
(c) The information and data held.

Systems may operate throughout the ship or may be limited to specific areas. They may be located entirely on-board, hosted by the Company or operate remotely. For example, the provision of satellite navigation signals.

In order to establish the nature of systems in use, the following questions will need to be answered:

(a) What ship systems are involved in the creation, use, maintenance, storage and transmission of ship data?
(b) To what extent are each of these systems dedicated to a single ship?
(c) Are the ship systems shared by different activities?
(d) Are the systems accessible by any third parties, aboard the ship, ashore, or on another ship?
(e) What is the typical operating life of each system?
(f) When is it likely that each system will become unsupportable, obsolete or need to be replaced for business and/or operational reasons? The channels by which systems, sensors and actuators communicate may be vulnerable to attacks and interference.

The answers to the following questions should therefore be obtained:
(a) What channels, technologies and parts of the overall spectrum are used to communicate and share ship data between ship systems and with any users who need to access or use it?
(b) What channels, technologies and parts of the electro-magnetic spectrum are used to control and integrate ship systems?
(c) To what extent are the communications confined to the ship, and will remote access to, or remote processing of, communications be required?

4.4 Mitigation

- 4.4.3 Implementation – Technology ll

GUIDANCE

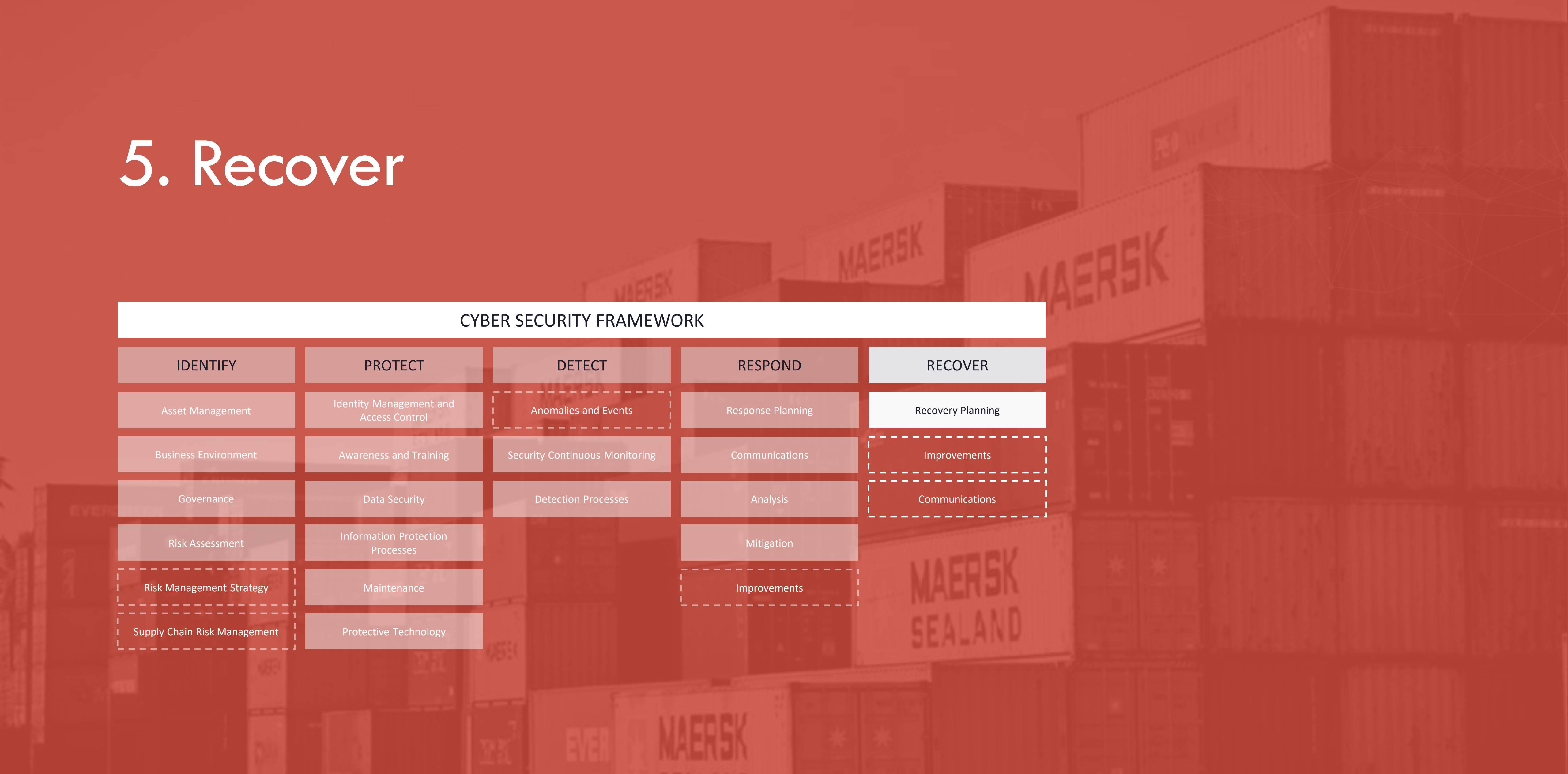
The information and data that is created, used and / or processed by the ship systems needs to be understood. In order to do this, the answers to the following questions should be established:

(a) What information and data, including sensor data, do the ship systems require to function?
(b) What other information and data is held? For example, Personally Identifiable Information
(c) What legal requirements are there with regards to the information and data held?
(d) How are information and data encoded?
(e) How and where are information and data stored?
(f) How is the data / information to be protected whilst at rest, in transit or in use?
(g) What will the consequences be if information and / or data was lost and therefore no longer available?
(h) Who owns the information and data?
(i) How are information and data made available and what restrictions are there on the use of the data?
(j) How long does information and data need to be kept?
(k) What information and data need to be securely removed when no longer required?

When designing, procuring, implementing and operating physical security systems that operate over IT, the SSO should consider how the systems will be protected from cyber security attacks or incidents. This is particularly important given the trend of convergence of systems. For example, the use of a shared network carrying operational data, administrative data and personal email traffic from shipboard personnel. Where such convergence occurs, or has occurred, the Company should ensure that:

(a) An appropriate architecture is employed;
(b) Appropriate management, support and maintenance is available from both the ship's engineering teams and the system vendors, to maintain system security and performance;
(c) Appropriate protection is provided to prevent IT control and security systems from being compromised;
(d) Wherever possible the critical security systems operate over a segregated infrastructure;
(e) Where appropriate encryption technology should be used to protect the data / information whilst at rest, in use or in transit.

5. Recover



CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

5.1 Recovery Planning

5.1 Recovery Planning

- 5.1.1 Controls

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 12.1 • 12.2 • 12.3 • 12.4 • 12.5 • 12.6	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	CP-10, IR-4, IR-8

5.1 Recovery Planning

- 5.1.2 Explanation

EXPLANATION

Resilience is the ability to adapt, respond and recover rapidly from disruptions and maintain continuity of business operations. In the event of an incident it is vital, from both a business and safety perspective, that a vessel is able to operate without disruption or compromise of the services provided to its crew and users.

Data recovery capability is the ability to restore a system and / or data from a secure copy or image. Thereby allowing the restoration of a clean system. Essential information and software backup facilities should be available to help ensure recovery following a cyber incident. Retention periods and restore scenarios should be established to prioritise which critical systems need rapid restore capabilities to reduce the impact. Systems that have high data availability requirements should be made resilient. OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident.

Additional goals for your cyber security recovery efforts may include, restoring information systems using alternate methods, performing standard operating procedures in alternate ways, recovering information systems in backup locations, and implementing contingency controls based on the business impact of the incident.

While it is preferable to avoid a cyber attack in the first place, the National Institute of Standards and Technology (NIST) notes that over-reliance on prevention is as bad as not being prepared. Some cyberattacks simply cannot be stopped, so focusing solely on prevention is a flawed approach.

Recovery plans should be available in hard copy on-board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To help ensure the safety of on-board personnel, the operation and navigation of the ship should be prioritised in the plan. The Recovery Plan should be understood by personnel responsible for cyber security. The detail and complexity of a Recovery Plan will depend on the type of ship and the IT, OT and other systems installed on-board.

The incident response team should consider carefully the implications of recovery actions (such as wiping of drives), which may result in the destruction of evidence that could provide valuable information as to the causes of an incident. Where possible, professional cyber incident response support should be obtained in order to assist in preservation of evidence whilst restoring operational capability.

Data recovery capabilities are normally in the form of software backup for IT data. The availability of a software backup, either on-board or ashore, should enable recovery of IT to an operational condition following a cyber incident. Recovery of OT may be more complex especially if there are no backup systems available and may require assistance from ashore. Details of where this assistance is available and by whom, should be part of the recovery plan. For example by proceeding to a port to obtain assistance from a service engineer. If qualified personnel are available on-board, more extensive diagnostic and recovery actions may be performed. Otherwise the recovery plan will be limited to obtaining quick access to technical support.

5.1 Recovery Planning

- 5.1.3 Implementation

GUIDANCE
A vessel should have a Security Incident Management Plan in place, which is based upon an understanding of: (a) The potential causes of disruption: cyber, human and natural; (b) The essential systems required to keep the vessel operating safely; (c) The nature and practicality of alternative methods which can be employed in the event of an incident to maintain operations; (d) The capacity at which the vessel can realistically operate under such arrangements. It will also be necessary for the vessel to have in place systems and processes which enable the timely detection of disruptive events, in order to enable the correct response as set out in the Security Incident Management plan, to be initiated as quickly as possible.
Emergency plans should be exercised on a regular basis, to test communication, coordination, resource availability, procedures and response. The exercises may be: (a) Full-scale or live; (b) Table-top simulation or seminar; or (c) Combined with other exercises such as emergency response, etc.
An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. (a) Checking back-up arrangements for critical systems, if not covered by existing procedures (b) Checking alternative modes of operation for critical systems, if not covered by existing procedures (c) Creating and obtaining back-up including clean images of OT to enable recovery from a cyber incident (d) Maintaining back-ups of data required for critical systems to operate safely (e) Offline storage of back-ups and clean images, if appropriate (f) Periodic testing of back-ups and back-up procedures

Appendix

MAERSK
MAERSK
MAERSK
MAERSK
MAERSK
MAERSK SEALAND
MAERSK
EVERGREEN

NIST Cyber Security Framework

- The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organisational risk management processes.

Explained

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The comprises five functions:

- Identify
- Protect
- Detect
- Respond
- Recover

These domains aid an organisation in executing and expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity.

Each function are further divided into categories and sub-categories.

Functions

Identify:
Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

Protect:
Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations..

Detect:
Develop and implement activities necessary to detect a cyber-event in a timely manner.

Respond:
Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Recover:
Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Application

The NIST Cyber Security Framework is used in combination with NIST SP 800-53 Rev. 4 and NIST SP 800-37.

In the framework, each function and its sub-categories are linked to a number of different controls from the control catalogue in NIST SP 800-53 Rev. 4. Based on the context of the organisation, these two publications can be used to determine the specific controls relevant.

NIST SP 800-37 can be used to facilitate the implementation of the Cyber Security framework. It demonstrated how the framework can be aligned with the Risk Management Framework and implemented using established NIST management processes.

NIST SP 800-53 Rev. 4

- The purpose of NIST SP 800-53 Rev. 4 is to heighten the security of information systems - the guidelines themselves apply to any component of an information system that stores, processes or transmits information.

Explained

The guidelines subdivides security controls into common, custom and hybrid categories:

- Common controls are those often used throughout an organisation.
- Custom controls are those intended to be used by an individual application or device.
- Hybrid controls start with a standard control and are customized per the requirements of a particular device or application.

The guidelines provides a catalog of controls that support the development of secure and resilient information systems

These are operational, technical and management safeguards used by information systems to maintain integrity, confidentiality and security of information systems

Controls

The controls are broken into 3 classes based on impact – low, moderate, and high – and split into 18 different families:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

Application

The guidelines introduces the concept of security control baselines as a starting point for the security control selection process.

These baselines outline a number of key considerations like operational and functional needs as well as the most common types of threats facing information systems.

A tailoring process is outlined too to help organisations select only those controls appropriate to the requirements of the information systems in use within their environment.

NIST guidelines adopt a multi-tiered approach to risk management through control compliance. SP 800-53 works alongside SP 800-37, which was developed to provide organisations with guidance on implementing risk management programs. SP 800-53 focuses on the controls which can be used along with the risk management framework outlined in 800-37.

NIST SP 800-37

- The purpose of NIST SP 800-37 is to provide guidelines for applying the Risk Management Framework (RMF) to information systems and organisations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk.

Explained

The Risk Management Framework includes activities to prepare organisations to execute the framework at appropriate risk management levels.

Promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes

Provides management with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions

Incorporates security and privacy into the system development life cycle.

Activities & Application

There are seven steps in the RMF; a preparatory step to ensure that organisations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF. The steps are:

- Prepare to execute the RMF from an organisation- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- Categorize the system and the information processed, stored, and transmitted by the system based on a security impact analysis.
- Select an initial set of controls for the system and tailor the controls as needed to mitigate risk based on an organisational assessment of risk and local conditions.
- Implement the controls and describe how the controls are employed within the system and its environment of operation.
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- Authorize the system or common controls based on a determination that the risk to organisational operations and assets, individuals, other organisations, and the Nation is acceptable.
- Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system

Resolution MSC.428(98)

- **Affirms** that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code
- **Encourages** administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021
- **Acknowledges** the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management
- **Request** Member States to bring this resolution to the attention of stakeholders
- IMO MSC-fal.1/Circ.3 5 July 2017:
- 1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these guidelines should refer to specific Member Governments' and Flag Administration's requirements, as well as relevant international and industry standards and best practice
- 2 High-level recommendations
- 2.2.3 guidelines are recommendatory

ISM Code

- Objective and functional requirements (for the SMS)

Objectives:

The objective of the Coda are to ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, in particular to the marine environment and to property.

1.2.2 Safety management objectives of the company should; inter alia:

.1 Provide for safe practices in shop operation and safe working environment;

.2 Assess all identified risks to its ship, personnel and the environment and establish appropriate safeguards;

.3 continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection

1.2.3 The safety management system should ensure:

.1 compliance with mandatory rules and regulations;

.2 that applicable codes, guidelines and standards recommended by the organization, administration, classification societies and maritime industry organisations are taken into account.

Functional requirements:

Every company should develop, implement and maintain a safety management system which includes the following functional requirements.

1.4 Functional requirements for a safety management system

- Safety and environmental-protection policy;
- Instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation;
- Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel
- Procedures for reporting accidents and non-conformities with the provisions of this code;
- Procedures to prepare for and respond to emergency situations;
- Procedures for internal audits and management reviews.

Mapping BIMCO Guidelines to NIST

CYBER SECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management 4, 5.1, 5.2, 5.3.3	Identity Management and Access Control 11.5 11.2	Anomalies and Events	Response Planning 7, 9.2, 9.3	Recovery Planning 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
Business Environment 1, 1.1, 1.2, 1.3	Awareness and Training 3, 5.6	Security Continuous Monitoring 5.5, 5.5.1, 5.5.2, 11.4	Communications 9.3	Improvements
Governance 2, 2.1, 2.2, 9, 9.1, 6, 8, 10	Data Security 6	Detection Processes 8	Analysis 9.4	Communications
Risk Assessment 5	Information Protection Processes 6, 11, 5.7		Mitigation 10	
Risk Management Strategy	Maintenance 11.1		Improvements	
Supply Chain Risk Management	Protective Technology 5.4, 11, 11.3, 5.3.4			

Digital Container Shipping Association

The DCSA Cyber Security is one of the main initiatives and publications of the DCSA.

VISION

The vision of the DCSA is to pave the way for interoperability in the container shipping industry through digitization and standardization. It is the DCSA's mission to represent, lead and serve the container shipping industry for safer, more secure and efficient operations of container shipping companies. The project track of the DCSA Information Model 1.0 in particular aims at increasing the level of common standards and designing a common language for processes, events, and messages.

MEMBERS

The Digital Container Shipping Association has the following members: CMA-CGM, Evergreen, Hapag-Lloyd, HMM, Maersk, MSC, ONE, Yang Ming and ZIM.

Contribution

The DCSA Implementation Guideline for BIMCO Compliant Cyber Security on Vessels will continue to be expanded with more practical guidance for the container shipping industry. This will be done based on ongoing collaboration with the industry.

CREATION PROCESS

The DCSA Information Model 1.0 has been made in collaboration with some of the world's largest shipping companies. The collection and consolidation of data documentation was carried out by the DSCA. The DCSA Information Model 1.0 aims at creating a representation of industry data references, data descriptions and data relationships.

SUGGESTED IMPROVEMENTS

The DCSA Information Model 1.0 will be a continually evolving document, which will change as processes and best practise across the industry change.
For this reason, the DCSA is always interested in feedback that can improve the quality of published work and drive standardization and digitalization going forward.
If you have any feedback or input, please go to our website under "Contact".

Thomas Bagge

CEO, DCSA

Henning Schleyerbach

COO, DCSA

www.dcsa.org

Follow us on LinkedIn

info@dcsa.org

@DCSA_ORG

Legal disclaimer