INTERNATIONAL MARITIME ORGANIZATION

E

FACILITATION COMMITTEE
40th session
Agenda item 9

FAL 40/INF.5
27 January 2016
ENGLISH ONLY

# GUIDELINES ON THE FACILITATION ASPECTS OF PROTECTING THE MARITIME TRANSPORT NETWORK FROM CYBERTHREATS

## Information on Cyber Risk Management Best Practices

**Submitted by Canada and the United States**

**SUMMARY**

| | |
|---|---|
| *Executive summary:* | This document presents an inventory of information security best practices to supplement ongoing efforts of the Committee to develop cyber risk management (CRM) guidelines for the protection of trade-related information |
| *Strategic direction:* | 6.1 |
| *High-level action:* | 6.1.1 |
| *Output:* | 6.1.1.2 |
| *Action to be taken:* | Paragraph 4 |
| *Related documents:* | FAL 39/7, FAL 39/WP.8, FAL 39/16; MSC 95/4/1, MSC 95/4/2, MSC 95/4/3, MSC 95/4/4, MSC 95/4/5, MSC 95/INF.19, MSC 95/22 and FAL 40/9 |


## Background

1 FAL 39 considered the proposal by Canada in documents FAL 39/7 and FAL 39/WP.8 to develop voluntary guidelines on cyber security practices to protect and enhance the resiliency of cyber systems supporting the operations of ports, vessels, facilities and other elements of the maritime transportation system. Additionally, at MSC 94 and 95 Canada, the United States, and other Member States and trade groups contributed submissions urging the development of cyber risk management (CRM) guidelines. Subsequently, Canada and the United States proposed the development of voluntary guidelines for consideration by the FAL Committee to address cyber-related risks on ships (see FAL 40/9). This information document provides an amalgamation of international CRM best practices that could serve as a point of reference for the elaboration and advancement of the guidelines proposed in the annex of FAL 40/9.

2 This document offers a range of information security best practices based on industry best practices and standards.

3 The best practices are organized into the same five categories as in FAL 40/9, for easier reference (i.e. Identification, Protection, Detection, Response, and Recovery).

**Action requested of the Committee**

4 The Committee is invited to note the information provided in this document.

***

# ANNEX

## FUNCTIONAL ELEMENTS

The Cyber Risk Management (CRM) outcomes and activities, articulated below, are built around the following five functional elements, which taken together can form the foundation of an effective CRM system:

1. **Identify**: processes aimed at defining personnel roles and responsibilities for CRM and identifying the systems, assets, data and capabilities that when disrupted pose risks to ship operations.

2. **Protect**: risk control processes and measures to protect against a cyber event and ensure continuity of shipping operations.

3. **Detect**: activities necessary to detect a cyber event in a timely manner.

4. **Respond**: response measures and processes to mitigate and contain a cyber event.

5. **Recover**: measures to back-up and restore cyber systems necessary for shipping operations impaired by a cyber event.

Achieving each functional element requires that certain outcomes be met. Outcomes, in turn, are met following the adoption of specific activities. This document highlights key outcomes associated with each functional element, as well as some of the key activities required to reach each outcome. Outcomes and activities were developed following a review of the following CRM-related publications:

- **ISO 27000** – ISO 27000 Series (Information Security Systems);

- **SANS** – The CIS Critical Security Controls for Effective Cyber Defense[1];

- **MITS** – Canada's Operational Security Standard: Management of Information Technology Standard;

- **INDUSTRY** – BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO developed The Guidelines on Cyber Security Onboard Ships; and

- **UCR** – Understanding Cyber Risk: Best Practices for Canada's Maritime Sector.

[1] The Center for Internet Security. (2015, October 15). *The CIS Critical Security Controls for Effective Cyber Defense.* Retrieved January 01, 2016, from Center for Internet Security: http://www.cisecurity.org/critical-controls.cfm

1 **IDENTIFY (ID)** could include the following outcomes:

.1 **Administrative Management (ID.AM)**: the resources and individuals that support critical functions are identified and managed consistent with effective CRM. The policies, procedures, and processes needed to inform and support ongoing CRM are also identified. To achieve effective administrative management owner/operators could:

| Activity | Informative Reference |
|---|---|
| (**ID.AM-1**) Design and implement an overarching CRM policy and communicate the policy to employees and third party-stakeholders as needed. | • **ISO 27001:2013** A.5.1.1, A.6.1.3, A.6.1.4, A.12.1.1<br>• **MITS** 9.2<br>• **INDUSTRY** 2.2, 3.1 |
| (**ID.AM-2**) Identify roles and responsibilities within the company necessary for effective CRM. | • **ISO 27001:2013** A.6.1.1<br>• **INDUSTRY** 2.3 |
| (**ID.AM-3**) Designate a person or persons for responsibility over the development, and regular review and evaluation of the CRM policy. | • **ISO 27001:2013** A.5.1.2<br>• **INDUSTRY** 2 |
| (**ID.AM-4**) Establish, maintain, communicate, and when necessary, enforce a disciplinary process for those who violate the CRM policy. | • **ISO 27001:2013** A.7.2.1, A.7.2.3 |
| (**ID.AM-5**) Review CRM policy at planned intervals or if significant changes occur. | • **ISO 27001:2013** A.5.1.2<br>• **UCR** AC.1, AC.2, AC.3 AC.8, GO.6<br>• **SANS** 3.1<br>• **MITS** 12.5, 12.12 |
| (**ID.AM-6**) Define cyber risk management responsibilities in employee and contractor agreements. | • **ISO 27001:2013** A.7.1.1, A.7.1.2, A.7.3.1,<br>• **UCR** SC.5, SC.9, SC.10 GO.17<br>• **SANS** 16.6<br>• **MITS** 12.6, 12.7<br>• **INDUSTRY** 4.2 |
| (**ID.AM-7**) Define cyber risk management responsibilities, expectations and rules in agreements with external parties. | • **ISO 27001:2013** A.13.1.2, A.13.2.2**,** A.14.1.1, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.2<br>• **ISO 27011** 6.2.3 |

.2 **Asset Management (ID.AS)**: systems, assets, data and capabilities are identified and managed consistent with effective CRM. To achieve effective asset management owner/operators could:

| Activity | Informative Reference |
|---|---|
| **(ID.AS-1)** Inventory and manage the use and allocation of physical devices and systems with a cyber nexus. | • **ISO 27001:2013** A.8.1.1, A.8.1.2, A.8.1.4<br>• **SANS** 1.1, 1.2, 1.3, 1.4, 2.1, 2.3 |
| **(ID.AS-2)** Map the connections (organizational communication and data flows) between inventoried systems. | • **ISO 27001:2013** A.13.2.1<br>• **SANS** 1.4, 2.3 |
| (**ID.AM-3**) Regularly review information systems for compliance with the organization's CRM policy. | • **ISO 27001:2013** A.18.2.3<br>• **INDUSTRY** 2.3 |

.3 **Risk Assessment (ID.RA)**: risks associated with cyber dependent systems are evaluated and prioritized. The company, vessel masters, and crew members understand potential cyber-related risks to operations, assets and individuals. To achieve an effective risk assessment owner/operators could:

| Activity | Informative Reference |
|---|---|
| (**ID.RA-1**) Identify and document potential threats to cyber assets. | • **INDUSTRY** 2.1, 3.3<br>• **ISO 27005:2011** 8.2.3 |
| (**ID.RA-2**) Identify and document cyber asset vulnerabilities. | • **INDUSTRY** 2.1, 3.3 |
| (**ID.RA-3**) Identify and document potential consequences due to failure or compromise of each cyber asset. | • **INDUSTRY** 2.1, 3.3<br>• **ISO 27005:2011** 8.2.6, 8.3.2<br>• **SANS** 13.1 |
| (**ID.RA-4**) Prioritize cyber assets based on potential threats, vulnerabilities, and consequences. | • **INDUSTRY** 2.1, 3.3<br>• **ISO 27005:2011** 8.1, 8.4<br>• **SANS** 13.1 |

2 **PROTECT (PR)** could include the following outcomes:

.1 **Access Control (PR.AC)**: criteria are established for whom or what may be granted authorized physical or electronic access to computer-based systems, databases or other records of information. Safeguards are established through processes, procedures and authorized activities to limit access to devices with a cyber nexus. To achieve effective access control owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.AC-1**) Manage the creation, use, and deletion of user and administrative accounts. Ensure that the principles of *least privilege* and *segregation of duties* are maintained. | • **ISO 27001:2013** A.6.1.2**,** A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A 9.4.2, A 9.4.3, A.9.4.4, A.9.4.5<br>• **INDUSTRY** 2.3, 3.13.3<br>• **SANS** 5.1, 5.2, 5.3, 5.6, 5.7, 5.9, 16.1, 16.2, 16.3, 16.4 |
| (**PR.AC-2**) Manage remote and wireless access to cyber systems and information to ensure access is provided only to appropriate personnel and devices. | • **INDUSTRY** 3.1<br>• **ISO 27001**:2013 A.6.2.2, A.13.1.1, A.13.2.1<br>• **SANS** 12.6, 12.7, 15.1, 15.2, 15.3, 15.4 |
| (**PR.AC-3**) Manage network integrity, incorporating network segregation and layered permissions where appropriate. Ensure the principle of *least privilege* is maintained. | • **ISO 27001:2013** A.13.1.1, A.13.1.3<br>• **ISO 27011** 6.2.2 |

| | |
|---|---|
| | • **ISO 27033-3** 8.3, 9.3<br>• **UCR** ND.7**,** SC.1<br>• **SANS** 1.5, 1.6, 9.1 9.2, 9.3, 9.4, 9.5, 9.6, 11.4, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.8, 12.9, 12.10, 13.6, 13.8, 14.1, 14.3, 14.4, 15.7, 15.9, 16.4<br>• **INDUSTRY** 3.1, 3.2, 3.3 |
| (**PR.AC-4**) Manage physical access to cyber systems and information to ensure access is provided only to appropriate personnel. | • **ISO 27001:2013** A.11.1.1, A.11.1.2, A.11.1.6<br>• **SANS** 11.5, 11.7,<br>• **MITS** 16.4.2, 16.4.6, 16.4.3<br>• **UCR** ND.1<br>• **INDUSTRY** 3.1, 3.2 |
| (**PR.AC-5**) Protect power and telecommunication cabling, and other information technology infrastructure from interception, interference or damage. | • **ISO 27001:2013** A.11.2.3, A.11.2.1, A.11.2.2<br>• **MITS** 16.4.10 |

.2 **Awareness and Training (PR.AT)**: personnel are provided CRM education and adequately trained to perform duties related to CRM. Personnel are aware of the cyber risks pertinent to their responsibilities and the safety and security of the ship. To achieve effective awareness and training owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.AT-1**) Train personnel in CRM and related roles and responsibilities. | • **ISO 27001:2013** A.7.2.2<br>• **SANS** 17.2<br>• **INDUSTRY** 1 |
| (**PR.AT-2**) Establish, maintain and enforce an information security awareness program to ensure employees and contractors receive information security training as appropriate to their responsibilities. | • **ISO 27001:2013** A.7.2.1, A.7.2.2<br>• **UCR** ND.3, GO.12, GO.15<br>• **SANS** 17.1, 17.2, 17.3, 17.4<br>• **MITS** 12.13<br>• **INDUSTRY** 1, 3.3 |
| (**PR.AT-3**) Define and communicate rules regarding the acceptable use of information. | • **ISO 27001:2013** A.8.1.3<br>• **SANS** 2.1 |
| (**PR.AT-4**) Define and implement a policy for protecting unattended workspaces and equipment. | • **ISO 27001:2013** A.11.2.8, A.11.2.9 |
| (**PR.AT-5**) Define and communicate rules regarding the acceptable use of removable media and mobile communication devices. | • **ISO 27001:2013** A.6.2.1, A.8.3.1, A.8.3.3<br>• **ISO 27033-3** 13.3<br>• **INDUSTRY** 2.3, 3.3 |

.3 **Data Integrity (PR.DI)**: information and records (data) are afforded a level of protection consistent with the overall cyber risk assessment strategy to protect the confidentiality, integrity, and availability of information. To achieve effective data integrity owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.DI-1**) Formally manage cyber-related assets throughout the lifecycle, transfers, and destruction or disposition. | • **ISO 27001:2013** A.6.1.5, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.14.2.5<br>• **ISO 27019:2013** 10.11<br>• **UCR** GO.5, GO.11, ND.5<br>• **MITS** 9.3, 9.10, 11, 12.1<br>• **INDUSTRY** 2, 3.2<br>• **SANS** 1.3, 4.5 |
| (**PR.DI-2**) Maintain adequate capacity and/or redundancy, Including back-ups, to ensure availability of data storage and transfer systems. | • **ISO 27001:2013** A.8.2.3, A.A.12.3.1, A.17.2.1<br>• **UCR** RE.7, ND8, SC.6<br>• **SANS** 10.1, 10.4, 3.2<br>• **INDUSTRY** 3.2, 3.3, 4.2 |
| (**PR.DI-3**) Implement measures to prevent data leaks, data loss and data destruction (including for back-ups). | • **ISO 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3. A.13.2.4, A.14.1.2, A.14.1.3 A.18.1.3<br>• **SANS** 10.3, 10.4, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 14.1, 14.2, 14.4, 14.5, 14.6, 14.7, 17.3<br>• **MITS** 13<br>• **UCR** ND.6 |
| (**PR.DI-4**) Establish safeguards to ensure the protection of data at-rest and in-transit. | • **ISO 27001:2013** A.8.2.3, A.10.1.1, A.10.1.2, A.13.1.1, A.13.2.1, A.13.2.2, A.13.2.3. A.13.2.4, A.14.1.2, A.14.1.3<br>• **INDUSTRY** 2.3, 3.3, 13.6, 13.7, 14.2, 14.4, 14.5, 15.5, 15.6 |
| (**PR.DI-5**) Define policy for papers, removable media, electronic displays, and unattended systems. | • **ISO 27001:2013** A.11.2.9 |
| (**PR.DI-6**) Manage the cyber risks associated with the off-site use of cyber systems. | • **ISO 27001:2013** A.11.2.5, A.11.2.6, A.6.2.2 |

.4 **Information Protection Processes and Procedures (PR.IP)**: security risk management processes and procedures are maintained and used to protect information systems and assets. To achieve effective information protection processes and procedures owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.IP-1**) Create and maintain a baseline configuration for information technology systems. | • **INDUSTRY** 2.3, 3.1, 3.3<br>• **ISO 27001:2013** A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4<br>• **SANS** 3.1, 3.2, 3.3, 3.6, 3.7. 7.1, 7.2, 7.3, 7.5, 7.6, 7.7, 9.1, 11.1, 11.2, 11.3, 11.6 |
| (**PR.IP-2**) Manage technical vulnerability assessments and associated remediation. | • **ISO 27001:2013** A.12.6.1<br>• **SANS** 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8<br>• **MITS** 12.5 |
| (**PR.IP-3**) Implement measures to manage the installation of software. | • **ISO 27001:2013** A.12.5.1, A.12.6.2.<br>• **SANS** 2.2, 2.4, 3.1, 7.1, 11.5, 11.6 |
| (**PR.IP-4**) Routinely evaluate and improve protection processes. | • **ISO 27001:2013** A.18.2.1, A.18.2.2 |

.5 **Maintenance (PR.MA)**: maintenance and repairs of control and information systems, as identified in section 1.2, are performed consistent with overarching cyber policies and procedures. To achieve effective maintenance owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.MA-1**) Perform timely asset maintenance and repair. Strictly control and manage access when conducting maintenance remotely. | • **ISO 27001:2013** A.11.2.4<br>• **SANS** 3.4, 3.5 |

.6 **Protective Technology (PR.PT)**: technical risk management solutions are implemented to ensure the integrity and resilience of cyber systems and assets including communications and control networks consistent with related policies, procedures and agreements. To achieve effective protective technology owner/operators could:

| Activity | Informative reference |
|---|---|
| (**PR.PT-1**) Log/audit records for protective technology are implemented and reviewed in accordance with company policy. | • **ISO 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1<br>• **SANS** 6.1, 6.2, 6.3, 7.4, 12.2, 14.6 |
| (**PR.PT-2**) Manage the use of removable media and external devices. | • **ISO 27001:2013** A.8.3.1<br>• **SANS** 8.3, 13.2, 13.5, 15.8, 15.9 |
| (**PR.PT-3**) Incorporate the principle of least functionality to control access to systems and assets. | • **ISO 27001:2013** A.9.1.1, A.9.1.2 |

| | |
|---|---|
| (**PR.PT-4**) Install, maintain and update anti-virus/anti-malware systems across the corporate network. | • **INDUSTRY** 3.1, 3.2<br>• **ISO 27001**:2013 A.12.2.1<br>• **SANS** 7.8, 8.1, 8.2, 8.4, 8.5. 8.6 |

3 **DETECT (DE)** could include the following outcomes:

.1 **Anomalies and Events (DE.AE)**: anomalous activity is detected in a timely manner and the potential impact of events is understood. To achieve effective anomalies and events owner/operators could:

| Activity | Informative reference |
|---|---|
| (**DE.AE-1**) Complete and maintain a baseline review of network operations and expected data flows for users and systems. | • **ISO 27039** 5.4.1, 5.4.2<br>• **SANS** 9.3, 12.2, 12.3 |
| (**DE.AE-2**) Establish incident alert thresholds. | • **SANS** 19.1, 19.4 |
| (**DE.AE-3**) Identify consequences of events. | • **ISO 27001:2013** A.16.1.4, A.16.1.4 |

.2 **Continuous Monitoring (DE.CM)**: cyber events are identified and verified to determine the effectiveness of protective measures. Information systems and assets are monitored to detect a cyber event in a timely manner. To achieve effective continuous monitoring owner/operators could:

| Activity | Informative reference |
|---|---|
| (**DE.CM-1**) Establish procedures to ensure networks are monitored to detect potential cyber events. | • **INDUSTRY** 3.2, 3.3<br>• **ISO 27001:2013** A.12.2.1, A 12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.6.1, A.14.2.7, A.15.2.1<br>• **SANS** 5.4, 5.5, 6.4, 6.5, 6.6, 12.2, 12.3, 12.8, 12.9, 12.10, 13.6, 13.7<br>• **UCR** ID.1, ID.2, ID.3<br>• **INDUSTRY** 3.2 |
| (**DE.CM-2**) Ensure the physical environment is monitored to detect potential cyber events. | • **ISO 27001:2013** A 11.1<br>• **ISO 27039** 5.4.7.1, 5.7, 5.8<br>• **INDUSTRY** 3.2 |
| (**DE.CM-3**) Maintain access control and user permissions. | • **ISO 27001:2013** A.9.1.1, A.9.1.2 |

.3 **Detection Processes (DE.DP)**: detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. To achieve effective detection processes owner/operators could:

| Activity | Informative reference |
|---|---|
| (**DE.DP-1**) Define roles and responsibilities for detection to ensure accountability. | • **ISO 27001:2013** A.16.1.3<br>• **INDUSTRY** 2.3 |
| (**DE.DP-2**) Test detection processes through periodic drills and exercises. | • **INDUSTRY** 3.2<br>• **SANS** 20.1 |
| (**DE.DP-3**) Communicate event detection information to appropriate parties. | • **ISO 27001:2013** A.6.1.4 |

4 **RESPOND (RE)**, could include the following outcomes:

.1 **Response Planning (RP)**: response processes and procedures are executed and maintained to ensure timely response to detected cyber events. To achieve effective response planning owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RE.RP-1**) Execute response plan during or after an event. | • **INDUSTRY** 2.3, 4, 4.1<br>• **ISO 27001:2013** A.16.1.2, A.6.1.1, A.6.1.3, A.16.1.5<br>• **SANS** 19-1, 19-2, 19-3, 19-4 |
| (**RE.RP-2**) Test response plan with periodic drills and exercises. | • **SANS** 19.7, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.8<br>• **ISO 27001:2013** A.17.1.3 |

.2 **Communications (RE.CO)**: response activities are coordinated with shipboard and external personnel. To achieve effective communications owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RE.CO-1**) Ensure personnel know their roles and order of operations when response is needed. | • **ISO 27001:2013** A.16.1.1<br>• **SANS** 19.1, 19.2, 19.3 |
| (**RE.CO-2**) Report events consistent with established criteria. | • **ISO 27001:2013** A.16.1.2<br>• **SANS** 19.4, 19.5 |
| (**RE.CO-3**) Share information with other vessels and companies to achieve broader cyber situational awareness. | • **ISO 27001:2013** A.6.1.4 |

.3 **Analysis (RE.AN)**: analysis is conducted to ensure adequate response and support recovery activities. To achieve effective analysis owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RE.AN-1**) Investigate notifications from detection systems. | • **MITS** 18.2<br>• **ISO 27001:2013** A.12.4.1, A.12.4.3, A.16.1.4, A.16.1.5<br>• **INDUSTRY** 2.3, 4 |
| (**RE.AN-2**) Analyse cyber-related incidents to understand the impact. | • **ISO 27001:2013** A.16.1.4, A.16.1.6 |
| (**RE.AN-3**) Perform forensics to prevent similar cyber events in the future. | • **ISO 27001:2013** A.16.1.7, A.16.1.6<br>• **MITS** 18.3, 18.6<br>• **INDUSTRY** 2.3, 4.3 |

.4 **Mitigation (RE.MI)**: activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. To achieve effective mitigation owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RE.MI-1**) Contain and mitigate cyber incidents to enable continuity of operations. | • **ISO 27001:2013** A.16.1.5 |
| (**RE.MI-2**) Mitigate, or document as accepted risks, newly identified vulnerabilities | • **ISO 27001:2013** A.12.6.1<br>• **SANS** 4.6, 4.7, 4.8 |

.5 **Improvements (RE.IM)**: incorporating lessons learned from current and previous detection/response activities as well as drills and exercises improves company response activities. To achieve effective improvements owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RE.IM-1**) Incorporate lessons learned into response plans. | • **ISO 27001:2013** A.16.1.6<br>• **SANS** 20.2, 20.7<br>• **INDUSTRY** 4.3 |
| (**RE.IM-2**) Update response strategies. | • **ISO 27001:2013** A.16.1.6 |

5 **RECOVER (RC)** could include the following outcomes:

.1 **Recovery Planning (RC.RP)**: recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber events. To achieve effective recovery planning owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RC.RP-1**) Establish processes and procedures to recover from cyber events. | • **ISO 27001:2013** A.17.1.1, A.17.1.2 |
| (**RC.RP-2**) Execute recovery plans during or after an event | • **INDUSTRY** 2.3,4.1<br>• **ISO 27001:2013** A.16.1.5 A.18.2.3<br>• **ISO 27031** 7.4.2<br>• **MITS** 18.5 |
| (**RC.RP-3**) Test recovery plans with regular exercises. | • **ISO 27001:2013** A.17.1.3 |

.2 **Improvements (RC.IM)**: recovery planning and processes are improved by incorporating lessons learned into future activities. To achieve effective improvements owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RC.IM-1**) Incorporate lessons learned into recovery plans. | • **ISO 27001:2013** A.16.1.6 |
| (**RC.IM-2**) Update recovery strategies. | • **ISO 27001:2013** A.17.1.3 |

.3 **Communications (RC.CO)**: restoration activities are coordinated with shipboard and external parties such as the ship's company, cargo owners, passengers or flag States. To achieve effective communications owner/operators could:

| Activity | Informative reference |
|---|---|
| (**RC.CO-1**) Manage public relations in accordance with company policy. | • **ISO 27001:2013** A.6.1.4, A.17.1.1, A.17.1.2 |
| (**RC.CO-2**) Communicate recovery activities to stakeholders. | • **ISO 27001:2013** A.6.1.3, A.6.1.4<br>• **SANS** 19.5 |