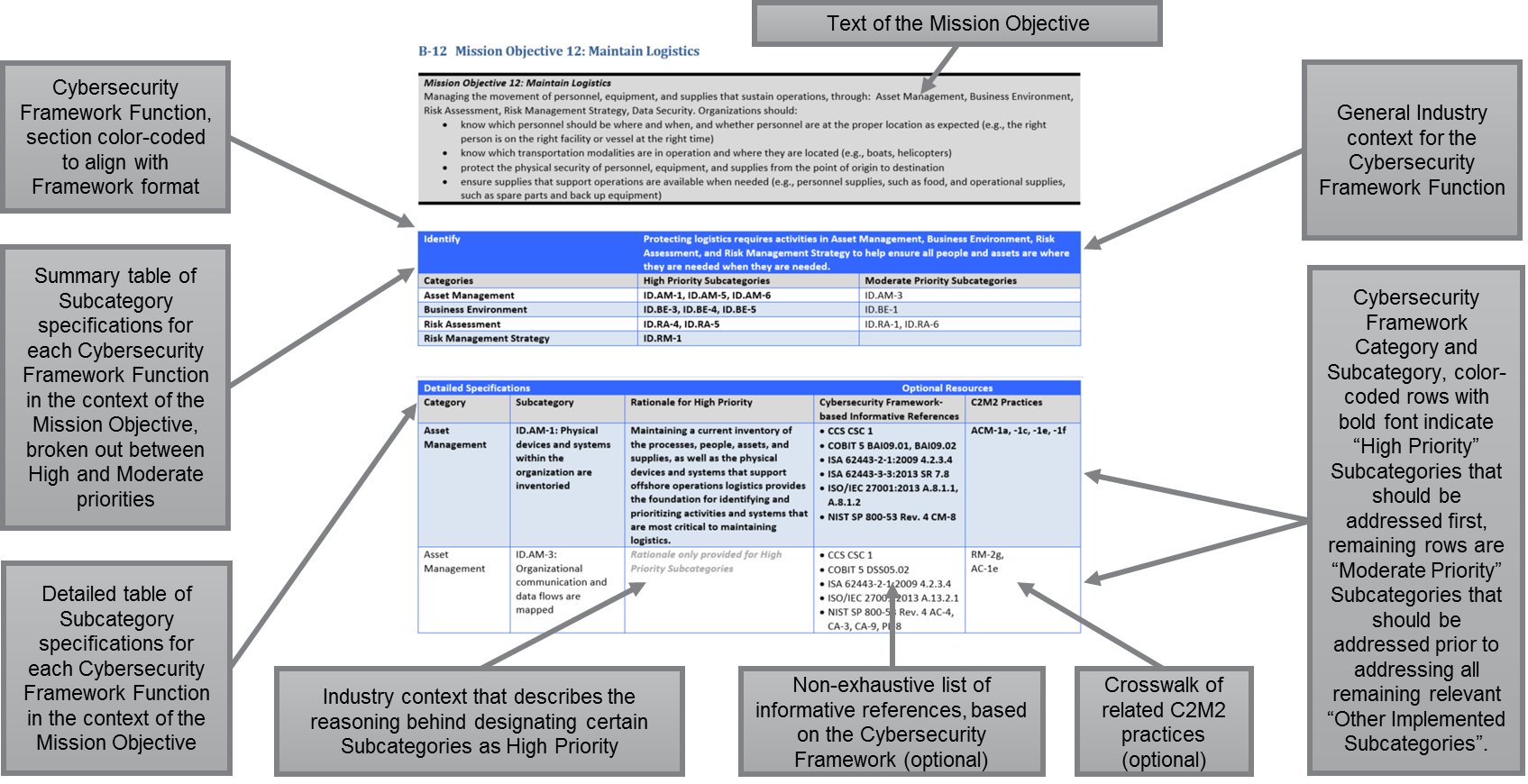
# Passenger Vessel Operations Profile

This Passenger Vessel Operations CFP defines the desired minimum state of cybersecurity by identifying the minimum set of Cybersecurity Framework Categories and Subcategories for each of the thirteen Mission Objectives required to conduct Passenger Vessel Operations in a more secure manner. Appendix C is divided into a subsection for each of the thirteen Mission Objectives listed in Section 7.5, Table 7-5 of the profile overview document. Each Mission Objective subsection in Appendix C includes both a summary and detailed table of High and Moderate Priority Subcategory specifications in the Profile by Cybersecurity Framework Function and Category. Figure C-1 provides a legend that describes the layout of the detailed Profile content provided.

Figure C‑1. Appendix C Content Legend



## **C-1 Mission Objective 1: Maintain Human Safety**

|  |
| --- |
| **Mission Objective 1 – Maintain Human Safety**  Recognizing cybersecurity effects on process control systems that impact personnel safety. Preventing injury, including loss of life, through Risk Assessment, Awareness and Training, Protective Technology, and Response Planning. Organizations should:  • account for all personnel on board active equipment  • understand scope of operational threats and their impacts to people  • manage risks to personnel using a structured process  • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact personnel safety  • implement Detect/Respond/Recover activities where cybersecurity adversely affects personnel safety |

|  |  |  |
| --- | --- | --- |
| Identify | Risk assessment processes are the primary methods used to identify procedures, technologies, and equipment that may impact the organization’s ability to maintain human safety. Each organization’s approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. | |
|  | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Risk Assessment | **ID.RA-3,** **ID.RA-5** | ID.RA-6 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Risk Assessment** | **ID.RA-3: Threats, both internal and external, are identified and documented** | **Understanding the threats that can impact the ability of IT and OT systems to operate reliably helps organizations manage risks accordingly, and plan for addressing potential incidents related to those specific threats if the risks associated with them are realized. ID.RA-3 assumes ID.RA-1 and ID.RA-2 are implemented.** | * **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** * **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** * **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16** | **TVM-1a, -1b, -1d, -1e, -1j**  **RM-2j** |
| **Risk Assessment** | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in a passenger vessel environment, as well as how the unique combination(s) of them affect the organization’s risk posture, is necessary for conducting thorough and accurate risk assessments and managing those risks in support of personnel safety needs. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.**  **Note that approaches to handling vulnerabilities may differ between IT and OT. IT vulnerabilities can often be patched. OT is not as easily patched, particularly when it is at risk of being taken offline. Additionally, patching OT may require a higher degree of vendor coordination to address needs of the equipment’s operating system and age.** | * **COBIT 5 APO12.02** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16** | **RM-1c, -2j,**  **TVM-2m** |
| Risk Assessment | ID.RA-6: Risk responses are identified and prioritized | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.05, APO13.02 * NIST SP 800-53 Rev. 4 PM-4, PM-9 * NIST SP 800-39 | RM-2e, 1c, -2j,  TVM-1d,  IR-3m |

|  |  |  |
| --- | --- | --- |
| Protect | Awareness and training, and protective technology were identified as the priority activities. Without awareness and training, personnel are not prepared to manage a personnel security incident. Without protective technology, systems will not be able to protect human life and deal with human safety issues. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1, PR.AT-3, PR.AT-5** |  |
| Protective Technology | **PR.PT-3** | **PR.PT-4** |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Awareness and Training** | **PR.AT-1: All users are informed and trained** | **Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related HR roles, responsibilities, and requirements necessary to support passenger vessel operations training accountability. Cybersecurity incidents can impact safety, making training critical for preventing personnel safety impacts.** | * **CCS CSC 9** * **COBIT 5 APO07.03, BAI05.07** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-2, PM-13** | **WM-3a, -4a, -3b, -3c,**  **-3d, -3g, -3h, -3i** |
| **Awareness and Training** | **PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities** | **Cybersecurity incidents can result from mistakes and other unintentional activities, not just malicious actors. Many passenger vessel operations rely heavily on a diverse staff to function. All personnel, regardless of which organization employs them directly, must understand how they may impact cybersecurity and behave accordingly in the context of the specific operations on their vessel.** | * **CCS CSC 9** * **COBIT 5 APO07.03, APO10.04, APO10.05** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 PS-7, SA-9** | **WM-1a, -1b, -1c, -1d,**  **-1e, -1f, -1g** |
| **Awareness and Training** | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in passenger vessel operations must understand the policies and procedures, including role descriptions, that are in place to address IT and OT cybersecurity risks that may result in personnel safety issues in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, physical and information security personnel must understand how to prioritize responsibilities as needed.**  **Note that PR.AT-5 assumes implementation of PR.AT-2.** | * **CCS CSC 9** * **COBIT 5 APO07.03** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-3, PM-13** | **WM-1a, -1b, -1c, -1d, -1e, -1f, -1g** |
| **Protective Technology** | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Provisioning physical and logical access based on the principle of least functionality/privilege limits access to resources to only those who need to access a system or asset and only those assets in the performance of their job duties. Those individuals should be provided adequate training to understand how to properly handle and maintain these assets, thereby limiting access by those who may inadvertently or intentionally cause harm to the assets.** | * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** * **ISO/IEC 27001:2013 A.9.1.2** * **NIST SP 800-53 Rev. 4 AC-3, CM-7** | **IAM-2a, -2b, -2c, -2d,**  **-2e, -2f, -2g, -2h, -2i** |
| Protective Technology | PR.PT-4: Communications and control networks are protected | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 7 * COBIT 5 DSS05.02, APO13.01 * ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 * ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 | CPM-3a, -3b, -3c, -3d |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

| Respond | Proper response plan development and execution is critical in the response phase of maintaining human safety. While strong focus on the Identify and Protection Functions helps prevent some incidents, it is still possible for incidents to occur, and organizations must be ready to handle them. | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Response Planning | **RS.RP-1** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Response Planning** | **RS.RP-1: Response plan is executed during or after an event** | **Response plans prepare organizations to respond effectively and efficiently when incidents occur. Responding appropriately to incidents can better protect the organization’s resources, including those that may impact personnel safety.** | * **COBIT 5 BAI01.10** * **CCS CSC 18** * **ISA 62443-2-1:2009 4.3.4.5.1** * **ISO/IEC 27001:2013 A.16.1.5** * **NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8** | **IR-3d** |

| Recover | N/A | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-2 Mission Objective 2: Maintain Marine Safety and Resilience**

|  |
| --- |
| **Mission Objective 2 – Maintain Marine Safety and Resilience**  Preserving systems integrity so that they function as designed and intended throughout their planned life helps maintain marine safety and resilience. Prevention of accidents and business impacts through Access Management, Risk Assessment; Risk Management and Response Planning. Organizations should:  • examine components that can cause failure alone or in combination  • design IT and OT integration points to "fail safe"  • preserve a steady state of containment when not in operation |

|  |  |  |
| --- | --- | --- |
| Identify | Access management, risk assessment, and risk management processes are the primary methods used to identify procedures, technologies, and equipment that may impact the organization’s ability to maintain marine safety and resilience. Each organization’s approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. | |
|  | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Management | **ID.AM-5, ID.AM-6** |  |
| Risk Assessment | **ID.RA-3,** **ID.RA-5** | ID.RA-1, ID.RA-6 |
| Risk Management | **ID.RM-3** | ID.RM-1 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Asset Management** | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Prioritizing resources is a necessary complement to inventory. Potential environmental safety impacts of passenger vessel systems are necessary factors to consider when prioritizing resources. For example, safety systems are among the highest priority resources, and taking them offline may lead to a failure to identify issues that can impact personnel. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed, with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |
| **Asset Management** | **ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established** | **Establishing and communicating cybersecurity roles and responsibilities is a fundamental requirement for enabling and effectively carrying out cybersecurity activities. As such, it is one of the first activities to address. Collaboration between points-of-contact (POCs) is important. At a minimum, consider defining roles and responsibilities for critical POCs.** | * **COBIT 5 APO01.02, DSS06.03** * **ISA 62443-2-1:2009 4.3.2.3.3** * **ISO/IEC 27001:2013 A.6.1.1** * **NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11** | **WM-1a, -1b, -1c** |
| Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 4 * COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 * ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 * ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 * NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | SA-1a,  IR-1C,  IAM-2a, -2b, -2c, 2d,  -2e, -2f, -2g, -2h |
| **Risk Assessment** | **ID.RA-3: Threats, both internal and external, are identified and documented** | **Understanding the threats that can impact the ability of IT and OT systems to operate reliably helps organizations manage risks accordingly, and plan for addressing potential incidents related to those specific threats if the risks associated with them are realized. ID.RA-3 assumes ID.RA-1 and ID.RA-2 are implemented.** | * **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** * **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** * **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16** | **TVM-1a, -1b, -1d, -1e, -1j,**  **RM-2j** |
| **Risk Assessment** | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in a passenger vessel environment, as well as how the unique combination(s) of them affect the organization’s risk posture, is necessary for conducting thorough and accurate risk assessments and managing those risks in support of personnel safety needs. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.**  **Note that approaches to handling vulnerabilities may differ between IT and OT.** **IT vulnerabilities can often be patched. OT is not as easily patched, particularly when it is at risk of being taken offline. Additionally, patching OT may require a higher degree of vendor coordination to address needs of the equipment’s operating system and age.** | * **COBIT 5 APO12.02** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16** | **RM-1c, -2j,**  **TVM-2m** |
| Risk Assessment | ID.RA-6: Risk responses are identified and prioritized | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.05, APO13.02 * NIST SP 800-53 Rev. 4 PM-4, PM-9 * NIST SP 800-39 | RM-2e, 1c, -2j,  TVM-1d,  IR-3m |
| Risk Management Strategy | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 * ISA 62443-2-1:2009 4.3.4.2 * NIST SP 800-53 Rev. 4 PM-9 | RM-1a, -1b, -1c, -1d,  -1e, -2a, -2b, -2c, -2d, -2e, 2g, -2h, -2j, -3a,  -3b, -3c, -3d, -3g, -3h,  -3i |
| Risk Management Strategy | **ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis** | **Critical infrastructure owners and operators maintain assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being. They are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient, ultimately supporting our Nation’s success. Protecting the environment is critical to the viability of continued passenger vessel operations. Operations that result in significant harms to the environment will be impeded or even halted, based on the severity of harms.**  **Note that ID.RM-3 assumes implementation of ID.RM-2.** | * **NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14** | **RM-1b, -1c** |

|  |  |  |
| --- | --- | --- |
| Protect | Maintenance and Protective Technology are required to maintain marine safety and resilience | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **Maintenance** | **PR.MA-1** | PR.MA-2 |
| **Protective Technology** | **PR.PT-3** | PR.PT-4 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Maintenance** | **PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools** | **Properly maintaining passenger vessel assets safeguards against preventable issues that could impact readiness and regulatory compliance. Managing maintenance through a defined approval process and with controlled tools protects the organization from introducing unnecessary risks, such as performing maintenance during a time that impacts other assets, changing implemented controls in a way that renders them ineffective, running tools that have not been scanned for malicious activity, or allowing access to unescorted and/or unauthorized individuals. For some assets, the ability to operate requires review and/or authorization and maintenance regimes by government regulators, standards bodies, or class societies.** | * **COBIT 5 BAI09.03** * **ISA 62443-2-1:2009 4.3.3.3.7** * **ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5**   **NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5** | **ACM-3b, -4c, -3f** |
| Maintenance | PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.04 * ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 * ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 * NIST SP 800-53 Rev. 4 MA-4 | SA-1a,  IR-1C,  IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h |
| **Protective Technology** | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Provisioning physical and logical access based on the principle of least functionality/privilege limits access to resources to only those who need to access a system or asset and only those assets in the performance of their job duties. Those individuals should be provided adequate training to understand how to properly handle and maintain these assets, thereby limiting access by those who may inadvertently or intentionally cause harm to the assets.** | * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** * **ISO/IEC 27001:2013 A.9.1.2** * **NIST SP 800-53 Rev. 4  AC-3, CM-7** | **IAM-2a, -2b, 2c, -2d,**  **-2e, -2f, -2g, -2h, -2i** |
| Protective Technology | PR.PT-4: Communications and control networks are protected | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 7 * COBIT 5 DSS05.02, APO13.01 * ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 * ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 | CPM-3a, -3b, -3c, -3d |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

| Respond | Proper response plan development and utilization is critical in the response phase of maintaining marine safety and resilience. | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Response Planning | **RS.RP-1** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| **Category** | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Response Planning** | **RS.RP-1: Response plan is executed during or after an event** | **Response plans prepare organizations to respond effectively and efficiently when incidents occur. Responding appropriately to incidents can help protect the organization’s resources, including those that may impact environmental safety.** | * **COBIT 5 BAI01.10** * **CCS CSC 18** * **ISA 62443-2-1:2009 4.3.4.5.1** * **ISO/IEC 27001:2013 A.16.1.5**   **NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8** | **IR-3d** |

| Recover | N/A | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-3 Mission Objective 3: Maintain Environmental Safety**

|  |
| --- |
| **Mission Objective 3: Maintain Environmental Safety**  Recognizing cybersecurity-effects on process control systems that impact environmental safety. Preventing harm to the environments and ecosystems through Governance, Risk Assessment, Awareness and Training, and Response Planning. Organizations should:   * account for all processes that may affect the environment * understand scope of operational threats and their potential adverse impacts to the environment * manage risks to the environment using a structured process * identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety * manage prominent and increasing role of automated systems in maintaining passenger vessel operations * implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety |

|  |  |  |
| --- | --- | --- |
| Identify | Governance and risk assessment processes are the primary methods used to identify risk identification and assessment processes that may impact the organization’s ability to maintain environmental safety. Each organization’s approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Governance | **ID.GV-3, ID.GV-4** |  |
| Risk Assessment | **ID.RA-3,** **ID.RA-5** | ID.RA-1, ID.RA-4, ID.RA-6 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Governance** | **ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed** | **Various passenger vessel activities may be driven or influenced by multiple laws, directives, policies, and regulations, including internal organizational policies that govern how information is collected and maintained by the organization. These requirements must be considered when developing internal and external stakeholder communications strategies.** | * **COBIT 5 MEA03.01, MEA03.04** * **ISA 62443-2-1:2009 4.4.3.7** * **ISO/IEC 27001:2013 A.18.1** * **NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)** | **AACM-4f,**  **CPM-2k,**  **EDM-3f,**  **IAM-3f,**  **IR-3n, -5f**  **ISC-2f,**  **RM-3f,**  **SA-4f,**  **TVM-3f,**  **WM-5f** |
| **Governance** | **ID.GV-4: Governance and risk management processes address cybersecurity risks** | **Governance and risk management processes support the organization’s implementation oflaws, directions, policies, and regulations, including internal organizational policies that address cybersecurity risks, thereby strengthening the security posture of the organization.**  **Cybersecurity risks can impact the organization’s operations, assets, individuals, business partners, and the Nation.** | * **COBIT 5 DSS04.02** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3** * **NIST SP 800-53 Rev. 4 PM-9, PM-11** | **RM-1c, -1e, -2a, -2b,**  **-2h, -3e** |
| Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* | * CCS CSC 4 * COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 * ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 * ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 * NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | SA-1a,  IR-1C,  IAM-2a, -2b, -2c, 2d,  -2e, -2f, -2g, -2h |
| **Risk Assessment** | **ID.RA-3: Threats, both internal and external, are identified and documented** | **Understanding the threats that can impact the ability of IT and OT systems to operate reliably helps organizations manage risks accordingly, and plan for addressing potential incidents related to those specific threats if the risks associated with them are realized. ID.RA-3 assumes ID.RA-1 and ID.RA-2 are implemented.** | * **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** * **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** * **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16** | **TVM-1a, -1b, -1d, -1e, -1j,**  **RM-2j** |
| Risk Assessment | ID.RA-4: Potential business impacts and likelihoods are identified | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 DSS04.02 * ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 * NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 | TVM-1d, -1f, -1c, 1i |
| **Risk Assessment** | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in a passenger vessel environment, as well as how the unique combination(s) of them affect the organization’s risk posture, is necessary for conducting thorough and accurate risk assessments and managing those risks in support of personnel safety needs. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.**  **Note that approaches to handling vulnerabilities may differ between IT and OT. IT vulnerabilities can often be patched. OT is not as easily patched, particularly when it is at risk of being taken offline. Additionally, patching OT may require a higher degree of vendor coordination to address needs of the equipment’s operating system and age.** | * **COBIT 5 APO12.02** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16** | **RM-1c, -2j,**  **TVM-2m** |
| Risk Assessment | ID.RA-6: Risk responses are identified and prioritized | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.05, APO13.02 * NIST SP 800-53 Rev. 4 PM-4, PM-9 * NIST SP 800-39 | RM-2e, 1c, -2j,  TVM-1d,  IR-3m |

|  |  |  |
| --- | --- | --- |
| Protect | Awareness and training is as well as a solid understanding of roles and responsibilities are critical to maintaining environmental safety. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1, PR.AT-5** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Awareness and Training** | **PR.AT-1: All users are informed and trained** | **Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related HR roles, responsibilities, and requirements necessary to support passenger vessel operations training accountability. Cybersecurity incidents can impact safety, making training critical for preventing personnel safety impacts.** | * **CCS CSC 9** * **COBIT 5 APO07.03, BAI05.07** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-2, PM-13** | **WM-3a, -4a, -3b, -3c,**  **-3d, -3g, -3h, -3i** |
| **Awareness and Training** | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in passenger vessel operations must understand the policies and procedures, including role descriptions, that are in place to address IT and OT cybersecurity risks that may result in personnel safety issues in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, physical and information security personnel must understand how to prioritize responsibilities as needed.**  **Note that PR.AT-5 assumes implementation of PR.AT-2.** | * **CCS CSC 9** * **COBIT 5 APO07.03** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-3, PM-13** | **WM-1a, -1b, -1c, -1d, -1e, -1f, -1g** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

| Respond | Proper response plan development and utilization is critical in the response phase of maintaining environmental safety. While strong focus on the Identify and Protection Functions helps prevent some incidents, it is still possible for incidents to occur, and organizations must be ready to handle them. | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Response Planning | **RS.RP-1** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Response Planning | **RS.RP-1: Response plan is executed during or after an event** | **Response plans prepare organizations to respond effectively and efficiently when incidents occur. Responding appropriately to incidents can help protect the organization’s resources, including those that may impact environmental safety.** | * **COBIT 5 BAI01.10** * **CCS CSC 18** * **ISA 62443-2-1:2009 4.3.4.5.1** * **ISO/IEC 27001:2013 A.16.1.5** * **NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8** | **IR-3d** |

| Recover | N/A | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-4 Mission Objective 4: Maintain Guest Support, Basic Hotel Services**

|  |
| --- |
| ***Mission Objective 4:* Maintain Guest Support, Basic Hotel Services**  Recognize cybersecurity effects on the guest support and hotel services aspect of a passenger vessel. Prevent harm to customers, the systems they use, employees, and services infrastructure such as booking, excursions, dining, entertainment, room service, and additional amenities. Organizations should:   * manage risk to all guest-facing systems * maintain account management security * manage support systems security * identify and securely protect guest personally identifiable information (PII) * control interfaces and data shared with business partners for ship entertainment, excursion, and hotel services |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management and risk assessment processes are the primary method used to identify assets, procedures, technologies, and risk processes that support the organization’s ability to maintain guest support and basic hotel services. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-5, ID.AM-6** | ID.AM-1, ID.AM-2 |
| Risk Assessment | **ID.RA-5,** **ID.RA-6** | ID.RA-3, ID.RA-4 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Asset Management | ID.AM-1: Physical devices and systems within the organization are inventoried | *Rationale only provided for High Priority Subcategories* | * CCS CSC 1 * COBIT 5 BAI09.01, BAI09.02 * ISA 62443-2-1:2009 4.2.3.4 * ISA 62443-3-3:2013 SR 7.8 * ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 * NIST SP 800-53 Rev. 4 CM-8 | ACM-1a, -1c, -1e, -1f |
| Asset Management | ID.AM-2: Software platforms and applications within the organization are inventoried | *Rationale only provided for High Priority Subcategories* | * CCS CSC 2 * COBIT 5 BAI09.01, BAI09.02, BAI09.05 * ISA 62443-2-1:2009 4.2.3.4 * ISA 62443-3-3:2013 SR 7.8 * ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 * NIST SP 800-53 Rev. 4 CM-8 | ACM-1a, -1c, -1e, -1f |
| Asset Management | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Understanding the inventory of software platforms and applications that support passenger vessel operations is critical to ensuring that vessel software is properly understood, supported, and maintained, as well as providing adequate visibility into operations.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |
| Asset Management | **ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established** | **Establishing and communicating cybersecurity roles and responsibilities is a fundamental requirement for enabling and effectively carrying out cybersecurity activities. As such, it is one of the first activities to address. Collaboration between points-of-contact (POCs) is important. At a minimum, consider defining roles and responsibilities for critical POCs.** | * **COBIT 5 APO01.02, DSS06.03** * **ISA 62443-2-1:2009 4.3.2.3.3** * **ISO/IEC 27001:2013 A.6.1.1** * **NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11** | **WM-1a, -1b, -1c** |
| Risk Assessment | ID.RA-3: Threats, both internal and external, are identified and documented | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 * ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 * NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 | TVM-1a, -1b, -1d, -1e, -1j,  RM-2j |
| Risk Assessment | ID.RA-4: Potential business impacts and likelihoods are identified | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 DSS04.02 * ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 * NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 | TVM-1d, -1f, -1c, 1i |
| **Risk Assessment** | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT technologies employed in a passenger vessel environment, as well as how the unique combination(s) of them affect the organization’s risk posture, is necessary for conducting thorough and accurate risk assessments and managing those risks in support of personnel safety needs. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.** | * **COBIT 5 APO12.02** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16** | **RM-1c, -2j,**  **TVM-2m** |
| **Risk Assessment** | **ID.RA-6: Risk responses are identified and prioritized** | **Impacts to the continuity and integrity of passenger vessel operations must be identified as such, and those implications must be considered in the prioritization given to risks in the organization’s risk response strategies. There are five basic types of responses to risk, with some overlap in between: (i) accept; (ii) avoid; (iii) mitigate; (iv) share; and (v) transfer.[[1]](#footnote-1) For risks that impact continuity and integrity of passenger vessel operations, “accept” may only be an appropriate option under limited circumstances.[[2]](#footnote-2) When choosing between Subcategories, addressing prioritized risks through ID.RA-6 is more important than formalizing risk management processes under ID.RM‑1, though organizations in higher Implementation Tiers are likely to also address ID.RM-1.** | * **COBIT 5 APO12.05, APO13.02** * **NIST SP 800-53 Rev. 4 PM-4, PM-9** * **NIST SP 800-39** | **RM-2e, 1c, -2j,**  **TVM-1d,**  **IR-3m** |

|  |  |  |
| --- | --- | --- |
| Protect | Awareness and training, protection processes and procedures and deployment of protective technology are critical to maintaining guest support and basic hotel services. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1, PR.AT-3, PR-AT-5** |  |
| Information Protection Processes & Procedures | **PR.IP-1, PR.IP-4**, **PR.IP-5** | PR.IP-3, PR.IP-11 |
| Protective Technology | **PR.PT-3, PR.PT-4** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Awareness and Training** | **PR.AT-1: All users are informed and trained** | **Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related HR roles, responsibilities, and requirements necessary to support passenger vessel operations training accountability. Cybersecurity incidents can impact safety, making training critical for preventing personnel safety impacts.** | * **CCS CSC 9** * **COBIT 5 APO07.03, BAI05.07** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-2, PM-13** | **WM-3a, -4a, -3b, -3c,**  **-3d, -3g, -3h, -3i** |
| **Awareness and Training** | **PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities** | **Cybersecurity incidents can result from mistakes and other unintentional activities, not just malicious actors. Many passenger vessel operations rely heavily on a diverse staff to function. All personnel, regardless of which organization employs them directly, must understand how they may impact cybersecurity and behave accordingly in the context of the specific operations on their vessel.** | * **CCS CSC 9** * **COBIT 5 APO07.03, APO10.04, APO10.05** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 PS-7, SA-9** | **WM-1a, -1b, -1c, -1d,**  **-1e, -1f, -1g** |
| **Awareness and Training** | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in passenger vessel operations must understand the policies and procedures, including role descriptions, that are in place to address cybersecurity risks that may result in personnel safety issues in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, physical and information security personnel must understand how to prioritize responsibilities as needed.**  **Note that PR.AT-5 assumes implementation of PR.AT-2.** | * **CCS CSC 9** * **COBIT 5 APO07.03** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-3, PM-13** | **WM-1a, -1b, -1c, -1d, -1e, -1f, -1g** |
| **Information Protection Processes & Procedures** | **PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained** | **Validated and tested baseline configurations promote consistency when configuring new systems and provide a reliable operating state. Baselines also support response and recovery efforts in returning to a reliable operating state after an incident. Organizations that need help getting started with baselines may choose to use available resources from security researchers, trade associations, standards bodies, and others, augmenting and tailoring those resources over time as they learn about their environment’s unique needs.** | * **CCS CSC 3, 10** * **COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** | **ACM-2a, -2b, -2c, -2d, -2e** |
| Information Protection Processes & Procedures | PR.IP-3: Configuration change control processes are in place | *Rationale only provided for High Priority Subcategories* | * COBIT 5 BAI06.01, BAI01.06 * ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 * ISA 62443-3-3:2013 SR 7.6 * ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 * NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 | ACM-3a, -3b, -3c, -3d, -4a, -3e, -3f, -4e |
| **Information Protection Processes and Procedures** | **PR.IP-4: Backups of information are conducted, maintained, and tested periodically** | **When cybersecurity incidents occur, good backups are one of the things that enable organizations to expediently return to a desirable state. Information backed up may also include user-level and system-level information. The confidentiality, integrity, and availability of backup media should be well protected to ensure that quality backups are available when needed. Testing should be periodically conducted to ensure that the technology is still available and usable to access the backup information and systems.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.9** * **ISA 62443-3-3:2013 SR 7.3, SR 7.4** * **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3** * **NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9** | **IR-4a, -4b** |
| **Information Protection Processes & Procedures** | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Policies and regulations provide a source of baseline expectations for the operating environment. Deviations in the physical operating environment could be an indication of cyber incidents, making awareness of policy and regulations an important input to cyber situational awareness.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** * **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18** | **ACM-4f,**  **RM-3f** |
| Information Protection Processes & Procedures | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 * ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 * ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 * NIST SP 800-53 Rev. 4 PS Family | WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h |
| **Protective Technology** | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Provisioning physical and logical access based on the principle of least functionality/privilege limits access to resources to only those who need to access a system or asset and only those assets in the performance of their job duties. Those individuals should be provided adequate training to understand how to properly handle and maintain these assets, thereby limiting access by those who may inadvertently or intentionally cause harm to the assets.** | * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** * **ISO/IEC 27001:2013 A.9.1.2** * **NIST SP 800-53 Rev. 4  AC-3, CM-7** | **IAM-2a, -2b, 2c, -2d,**  **-2e, -2f, -2g, -2h, -2i** |
| **Protective Technology** | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to passenger vessel assets. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in operational security issues.** | * **CCS CSC 7** * **COBIT 5 DSS05.02, APO13.01** * **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** * **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7** | **CPM-3a, -3b, -3c, -3d** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | **N/A** | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-5 Mission Objective 5: Maintain Regulatory Compliance**

|  |
| --- |
| ***Mission Objective 5: Maintain Regulatory Compliance***  Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Asset Management, Governance, Risk Management, and Awareness and Training. Organizations should:  • track regulatory activity and assess impacts to operations  • incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures  • develop ongoing relationships with regulators  • ensure that foundational “cyber hygiene” activities are addressed as part of the overall risk management program  • contribute to industry standards and best practices |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management, governance, risk assessment, and risk management processes are the primary methods used to identify procedures, technologies, and equipment that support the organization’s ability to maintain regulatory compliance. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-1, ID.AM-2, ID.AM-5** | ID.AM-6 |
| Governance | **ID.GV-3, ID.GV-4** | ID.GV-1, ID.GV-2 |
| Risk Management Strategy | **ID.RM-1, ID.RM-3** | ID.RM-2 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Asset Management** | **ID.AM-1: Physical devices and systems within the organization are inventoried** | **Maintaining a current inventory of the physical devices and systems that support passenger vessel operations provides the foundation for identifying and prioritizing assets that are most critical to maintaining the continuity and integrity of operations.** | * **CCS CSC 1** * **COBIT 5 BAI09.01, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.4** * **ISA 62443-3-3:2013 SR 7.8** * **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** * **NIST SP 800-53 Rev. 4 CM-8** | **ACM-1a, -1c, -1e, -1f** |
| **Asset Management** | **ID.AM-2: Software platforms and applications within the organization are inventoried** | **Understanding the inventory of software platforms and applications that support passenger vessel operations is critical to ensuring that vessel software is properly understood, supported, and maintained, as well as providing adequate visibility into operations.** | * **CCS CSC 2** * **COBIT 5 BAI09.01, BAI09.02, BAI09.05** * **ISA 62443-2-1:2009 4.2.3.4** * **ISA 62443-3-3:2013 SR 7.8** * **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** * **NIST SP 800-53 Rev. 4 CM-8** | **ACM-1a, -1c, -1e, -1f** |
| **Asset Management** | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Prioritizing resources is a necessary complement to inventory. Potential environmental safety impacts of passenger vessel systems are necessary factors to consider when prioritizing resources. For example, safety systems are among the highest priority resources, and taking them offline may lead to a failure to identify issues that can impact personnel. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |
| Asset Management | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO01.02, DSS06.03 * ISA 62443-2-1:2009 4.3.2.3.3 * ISO/IEC 27001:2013 A.6.1.1 * NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 | WM-1a, -1b, -1c |
| Governance | ID.GV-1: Organizational information security policy is established | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO01.03, EDM01.01, EDM01.02 * ISA 62443-2-1:2009 4.3.2.6 * ISO/IEC 27001:2013 A.5.1.1 * NIST SP 800-53 Rev. 4 -1 controls from all families | CPM-2g, -5d,  RM-3e |
| Governance | ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.12 * ISA 62443-2-1:2009 4.3.2.3.3 * ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 * NIST SP 800-53 Rev. 4 PM-1, PS-7 | WM-1a, -1b, -1c, -1e,  -1f, -1g, -2d, -5b,  ISC-2b |
| **Governance** | **ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed** | **Various passenger vessel activities may be driven or influenced by multiple laws, directives, policies, and regulations, including internal organizational policies, that govern how information is collected and maintained by the organization. These requirements must be considered when developing internal and external stakeholder communications strategies.** | * **COBIT 5 MEA03.01, MEA03.04** * **ISA 62443-2-1:2009 4.4.3.7** * **ISO/IEC 27001:2013 A.18.1** * **NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)** | **AACM-4f,**  **CPM-2k,**  **EDM-3f,**  **IAM-3f,**  **IR-3n, -5f**  **ISC-2f,**  **RM-3f,**  **SA-4f,**  **TVM-3f,**  **WM-5f** |
| **Governance** | **ID.GV-4: Governance and risk management processes address cybersecurity risks** | **Governance and risk management processes support the organization’s implementation oflaws, directions, policies, and regulations, including internal organizational policies that address cybersecurity risks, thereby strengthening the security posture of the organization.**  **Cybersecurity risks can impact the organization’s operations, assets, individuals, business partners, and the Nation.** | * **COBIT 5 DSS04.02** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3** * **NIST SP 800-53 Rev. 4 PM-9, PM-11** | **RM-1c, -1e, -2a, -2b,**  **-2h, -3e** |
| **Risk Management Strategy** | **ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders** | **Addressing risks to continuity and integrity of passenger vessel operations in accordance with risk management strategies requires clearly defined procedures and engaged stakeholders that understand their roles in executing risk management activities. Documenting activities and roles allows all stakeholders to: (i) come to a common understanding of the risks and risk management processes, (ii) collaboratively determine the most effective ways to integrate risk management processes into the operational environment, and (iii) understand the responsibilities for which they are held accountable.** | * **COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02** * **ISA 62443-2-1:2009 4.3.4.2** * **NIST SP 800-53 Rev. 4 PM-9** | **RM-1a, -1b, -1c, -1d,**  **-1e, -2a, -2b, -2c, -2d, -2e, 2g, -2h, -2j, -3a,**  **-3b, -3c, -3d, -3g, -3h,**  **-3i** |
| Risk Management Strategy | ID.RM-2: Organizational risk tolerance is determined and clearly expressed | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 APO12.06 * ISA 62443-2-1:2009 4.3.2.6.5 * NIST SP 800-53 Rev. 4 PM-9 | RM-1c, -1e |
| **Risk Management Strategy** | **ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis** | **Critical infrastructure owners and operators maintain assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being. They are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient, ultimately supporting our Nation’s success. Protecting the environment is critical to the viability of continued passenger vessel operations. Operations that result in significant harms to the environment will be impeded or even halted, based on the severity of harms.**  **Note that ID.RM-3 assumes implementation of ID.RM-2.** | * **NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14** | **RM-1b, -1c** |

|  |  |  |
| --- | --- | --- |
| Protect | Proper awareness and training are key to maintaining regulatory compliance. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1, PR.AT-3** | PR.AT-4, PR.AT-5 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Awareness and Training** | **PR.AT-1: All users are informed and trained** | **Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity- roles, responsibilities, and requirements necessary to support passenger vessel operations.** | * **CCS CSC 9** * **COBIT 5 APO07.03, BAI05.07** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-2, PM-13** | **WM-3a, -4a, -3b, -3c,**  **-3d, -3g, -3h, -3i** |
| **Awareness and Training** | **PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities** | **Cybersecurity incidents can result from mistakes and other unintentional activities, not just malicious actors. Many passenger vessel operations rely heavily on a diverse staff to function. All personnel, regardless of which organization employs them directly, must understand how they may impact cybersecurity and behave accordingly in the context of the specific operations on their vessel.** | * **CCS CSC 9** * **COBIT 5 APO07.03, APO10.04, APO10.05** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 PS-7, SA-9** | **WM-1a, -1b, -1c, -1d,**  **-1e, -1f, -1g** |
| Awareness and Training | PR.AT-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9 * COBIT 5 APO07.03 * ISA 62443-2-1:2009 4.3.2.4.2 * ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 * NIST SP 800-53 Rev. 4 AT-3, PM-13 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Awareness and Training | PR.AT-5: Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9 * COBIT 5 APO07.03 * ISA 62443-2-1:2009 4.3.2.4.2 * ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 * NIST SP 800-53 Rev. 4 AT-3, PM-13 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | **N/A** | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | **N/A** | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-6 Mission Objective 6: Assure Secure Communications by Function and Mode**

|  |
| --- |
| ***Mission Objective 6: Assure Communications by Function and Mode***  Ensuring that communications required to operate positioning equipment and ship-to-shore communications are available reliably. Protecting communications channels through Risk Assessment, Data Security, Information Protection Processes and Procedures, Protective Technology, Anomaly and Event Detection, and Security Continuous Monitoring. Organizations should:  • understand communication flows between ship and shore  • protect integrity of positioning equipment and other equipment that can be affected remotely  • protect personal information |

|  |  |  |
| --- | --- | --- |
| Identify | Risk assessment processes are the primary methods used to identify procedures, technologies, and equipment that support the organization’s ability to assure secure communications. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Risk Assessment | **ID.RA-3, ID.RA-5, ID.RA-6** | ID.RA-1 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* | * CCS CSC 4 * COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 * ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 * ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 * NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | SA-1a,  IR-1C,  IAM-2a, -2b, -2c, 2d,  -2e, -2f, -2g, -2h |
| **Risk Assessment** | **ID.RA-3: Threats, both internal and external, are identified and documented** | **Understanding the threats that can impact the ability of IT and OT systems to operate reliably helps organizations manage risks accordingly, and plan for addressing potential incidents related to those specific threats if the risks associated with them are realized. ID.RA-3 assumes ID.RA-1 and ID.RA-2 are implemented.** | * **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** * **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** * **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16** | **TVM-1a, -1b, -1d, -1e, -1j,**  **RM-2j** |
| **Risk Assessment** | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in a passenger vessel environment, as well as how the unique combination(s) of them affect the organization’s risk posture, is necessary for conducting thorough and accurate risk assessments and managing those risks in support of personnel safety needs. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.**  **Note that approaches to handling vulnerabilities may differ between IT and OT. IT vulnerabilities can often be patched. OT is not as easily patched, particularly when it is at risk of being taken offline. Additionally, patching OT may require a higher degree of vendor coordination to address needs of the equipment’s operating system and age.** | * **COBIT 5 APO12.02** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16** | **RM-1c, 2j,**  **TVM-2m** |
| **Risk Assessment** | **ID.RA-6: Risk responses are identified and prioritized** | **Impacts to the continuity and integrity of passenger vessel operations must be identified as such, and those implications must be considered in the prioritization given to risks in the organization’s risk response strategies. There are five basic types of responses to risk, with some overlap in between: (i) accept; (ii) avoid; (iii) mitigate; (iv) share; and (v) transfer.[[3]](#footnote-3) For risks that impact continuity and integrity of passenger vessel operations, “accept” may be an appropriate option only under limited circumstances.[[4]](#footnote-4) When choosing between Subcategories, addressing prioritized risks through ID.RA-6 is more important than formalizing risk management processes under ID.RM‑1, though organizations in higher Implementation Tiers are likely to also address ID.RM-1.** | * **COBIT 5 APO12.05, APO13.02** * **NIST SP 800-53 Rev. 4 PM-4, PM-9** | **RM-2e, 1c, -2j,**  **TVM-1d,**  **IR-3m** |

| Protect | Maintaining cyber situational awareness in passenger vessel operations requires data security, supporting processes and procedures, and protective technologies to assure secure communications. | |
| --- | --- | --- |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Data Security | **PR.DS-2, PR.DS-4, PR.DS-5** | PR.DS-3 |
| Information Protection Processes and Procedures | **PR.IP-3, PR.IP-4, PR.IP-9** | PR.IP-1 |
| Protective Technology | **PR-PT-3, PR.PT-4** | PR.PT-1 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Data Security** | **PR.DS-2: Data-in-transit is protected** | **IT and OT data must be protected as it travels across internal and external networks, particularly external networks where it may be subject to interception or modification.** | * **CCS CSC 17** * **COBIT 5 APO01.06, DSS06.06** * **ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2** * **ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3** * **NIST SP 800-53 Rev. 4 SC-8** | **TVM-1c, -2c** |
| Data Security | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition | *Rationale only provided for High Priority Subcategories* | * COBIT 5 BAI09.03 * ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 * ISA 62443-3-3:2013 SR 4.2 * ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 * NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 | ACM-3a, -3b, -3c, -3d,  -3f, -4a, -4b, -4c, -4d,  -4e, -4f, -4g |
| **Data Security** | **PR.DS-4: Adequate capacity to ensure availability is maintained** | **Capacity planning is conducted to identify and address threats to passenger vessel operations. Maintaining adequate capacity ensures that essential mission and business functions continue running efficiently and may reduce susceptibility to denial of service attacks.** | * **COBIT 5 APO13.01** * **ISA 62443-3-3:2013 SR 7.1, SR 7.2** * **ISO/IEC 27001:2013 A.12.3.1** * **NIST SP 800-53 Rev. 4  AU-4, CP-2, SC-5** | **TVM-1c, -2c**  **CPM-3b** |
| **Data Security** | **PR.DS-5: Protections against data leaks are implemented** | **Communications can relay valuable information about the health of IT and OT activities, proprietary and safety information about instructions for handling incidents, and other sensitive information. Leaks of this information could range in impact due to a loss of control of the information.**  **Security categories or classifications of information influence the level of protections implemented to protect the communications channels and the information that flows across them.** | * **CCS CSC 17** * **COBIT 5 APO01.06** * **ISA 62443-3-3:2013 SR 5.2** * **ISO/IEC 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** * **NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4** | **CPM-3b**  **TVM-1c, -2c, -2n** |
| Information Protection Processes & Procedures | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained | *Rationale only provided for High Priority Subcategories* | * CCS CSC 3, 10 * COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 * ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 * ISA 62443-3-3:2013 SR 7.6 * ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 * NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 | ACM-2a, -2b, -2c, -2d, -2e |
| **Information Protection Processes & Procedures** | **PR.IP-3: Configuration change control processes are in place** | **Change control processes provide a structured approach to managing changes to existing systems, ensuring that each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports reliability by limiting the potential for unplanned changes and managing planned changes in accordance with decisions previously made, as well as vetted organizational requirements and standards to limit adverse impacts.** | * **COBIT 5 BAI06.01, BAI01.06** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10** | **ACM-3a, -3b, -3c, -3d, -4a, -3e, -3f, -4e** |
| **Information Protection Processes and Procedures** | **PR.IP-4: Backups of information are conducted, maintained, and tested periodically** | **When cybersecurity incidents occur, good backups are one of the things that enable organizations to expediently return to a desirable state. Information backed up may also include user-level and system-level information. The confidentiality, integrity, and availability of backup media should be well protected to ensure that quality backups are available when needed. Testing should be periodically conducted to ensure that the technology is still available and usable to access the backup information and systems.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.9** * **ISA 62443-3-3:2013 SR 7.3, SR 7.4** * **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3** * **NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9** | **IR-4a, -4b** |
| **Information Protection Processes and Procedures** | **PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed** | **Passenger vessel operations response and recovery plans define the degree of IT and OT operations necessary to return to a desired minimum state of operations after a cybersecurity event. Developing and managing these plans in coordination with incident response processes ensures that the necessary activities occur when a cybersecurity event is identified. Instituting processes to manage response and recovery plans ensures that they are periodically updated, allowing the organization to maintain an acceptable level of preparedness. This activity supports response and recovery activities so that passenger vessel operations can return to a desirable state expediently.**  **Note that PR.IP-9 assumes PR.IP-10 is addressed. Note also, PR.IP-9 and PR.IP-12 should be developed and maintained with coordination.** | * **COBIT 5 DSS04.03** * **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** * **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2** * **NIST SP 800-53 Rev. 4 CP-2, IR-8** | **IR-4c, -3f, -4d. -4f, -5a, -5b, -5d, -3k, -3m, -4j, -5e, -5f, -5g, -5h, -5i,**  **TVM-1d,**  **RM-1c** |
| Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | *Rationale only provided for High Priority Subcategories* | * CCS CSC 14 * COBIT 5 APO11.04 * ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 * ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 * ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 * NIST SP 800-53 Rev. 4 AU Family | SA-1a, -1b, -1c, -2a,  -2e, -3d, -4e, -4f, -4g |
| **Protective Technology** | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Provisioning physical and logical access based on the principle of least functionality/privilege limits access to resources to only those who need to access a system or asset and only those assets in the performance of their job duties. Those individuals should be provided adequate training to understand how to properly handle and maintain these assets, thereby limiting access by those who may inadvertently or intentionally cause harm to the assets.** | * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** * **ISO/IEC 27001:2013 A.9.1.2** * **NIST SP 800-53 Rev. 4 AC-3, CM-7** | **IAM-2a, -2b, -2c, -2d,**  **-2e, -2f, -2g, -2h, -2i** |
| **Protective Technology** | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to passenger vessel assets. For example, information about OT assets may be sent to an onshore facility for monitoring. This access can provide useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in operational security issues.** | * **CCS CSC 7** * **COBIT 5 DSS05.02, APO13.01** * **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** * **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7** | **CPM-3a, -3b, -3c, -3d** |

|  |  |  |
| --- | --- | --- |
| Detect | Anomaly detection processes and continuous monitoring activities to identify anomalies and events are critical aspects of assuring secure communications. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-1, DE.AE-4, DE.AE-5** |  |
| Security Continuous Monitoring | **DE.CM-1, DE.CM-6, DE.CM-7** | DE.CM-3, DE.CM-5 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Anomalies and Events** | **DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed** | **Understanding the baseline of network operations and expected data flows during passenger vessel operations supports operational security by providing a means of comparing current activities against expectations to identify anomalies or other events that may require analysis and response.** | * **COBIT 5 DSS03.01** * **ISA 62443-2-1:2009 4.4.3.3** * **NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4** | **SA-2a** |
| **Anomalies and Events** | **DE.AE-4: Impact of events is determined** | **Knowing the impact of events helps organizations understand the impact to maintaining the integrity and continuity of passenger vessel operations, how to appropriately respond, and what measures may be necessary to recover from the event.** | * **COBIT 5 APO12.06** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4** | **IR-2b, -2d, -2g, -2j,**  **TVM-1d** |
| **Anomalies and Events** | **DE.AE-5: Incident alert thresholds are established** | **Determining incident alert thresholds that support maintaining cyber situational awareness will help ensure that the organization reacts appropriately and in a timely manner when incidents are detected.** | * **COBIT 5 APO12.06** * **ISA 62443-2-1:2009 4.2.3.10** * **NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8** | **IR-2a, -2d, -2g,**  **TVM-1d, SA-2d, RM-2j** |
| **Security Continuous Monitoring** | **DE.CM-1: The network is monitored to detect potential cybersecurity events** | **Monitoring is a foundational activity for discovering cybersecurity events that may impact passenger vessel operations communications.** | * **CCS CSC 14, 16** * **COBIT 5 DSS05.07** * **ISA 62443-3-3:2013 SR 6.2** * **NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4** | **SA-2a, -2**  **b, 2e, -2f, -2g, -2i,**  **TVM-1d** |
| Security Continuous Monitoring | DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-3-3:2013 SR 6.2 * ISO/IEC 27001:2013 A.12.4.1 * NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 | SA-2a, -2b, -2e, -2i |
| Detection Processes | DE.CM-5: Unauthorized mobile code is detected | ***Rationale only provided for High Priority Subcategories*** | ISA 62443-3-3:2013 SR 2.4  ISO/IEC 27001:2013 A.12.5.1  NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 |  |
| **Security Continuous Monitoring** | **DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events** | **Monitoring external service provider activity for access issues and other issues is one of the primary ways to maintain cyber situational awareness and identify anomalies that can lead to cybersecurity events with adverse impacts. DE.CM-6 assumes DE.CM 1‑5 are covered.** | * **COBIT 5 APO07.06** * **ISO/IEC 27001:2013 A.14.2.7, A.15.2.1** * **NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4** | **EDM-2a, -2j, -2n,**  **SA-2a, -2b, -2e** |
| **Security Continuous Monitoring** | **DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed** | **Monitoring for unauthorized activities supports operational security by identifying events, in accordance with defined monitoring objectives that may signify a cybersecurity issue, and providing the necessary information to support an appropriate risk response. Outputs from monitoring passenger vessel operations provide input into event correlation and analysis tools, alert mechanisms, and the response process. DE.CM-7 assumes DE.CM 1-5 are covered.** | * **NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4** | **SA-2a, -2b, -2e, -2f,**  **-2g, -2i,**  **TVM-1d** |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

## **C-7 Mission Objective 7: Optimize and Enhance Guest Experience and Value**

|  |
| --- |
| ***Mission Objective 7:* Optimize and Enhance Guest Experience and Value**  Recognize cybersecurity role in the guest experience. Prevent harm to customers in booking, excursions, dining, entertainment, room service, and additional amenities. The organization should:   * provide seamless interface to guests as they request services * manage support systems security * identify and securely protect guest personally identifiable information (PII) * manage interfaces and data shared with business partners for ship entertainment, excursion, and hotel services |

|  |  |  |
| --- | --- | --- |
| Identify | The business environment is the most relevant category for optimizing the guest experience and value. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-3, ID.BE-4, ID.BE-5** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Business Environment** | **ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated** | **Effectively protecting passenger vessel operations assets depends on stakeholder awareness of the organization’s mission and objectives, and how those things influence their activities, both generally and specifically, for properly managing and protecting the priority systems and assets of the organization.** | * **COBIT 5 APO02.01, APO02.06, APO03.01** * **ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6** * **NIST SP 800-53 Rev. 4 PM-11, SA-14** | **RM-1c, -3b** |
| **Business Environment** | **ID.BE-4: Dependencies and critical functions for delivery of critical services are established** | **Dependency and criticality analysis informs protection activities that are critical to maintaining the passenger vessel operations activities required for operational efficiency. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated operational functions and activities, as well as traceability to specific assets.** | * **ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3** * **NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14** | **ACM-1a, -1b, -1c, -1d, -1e, -1f,**  **EDM-1a, -1c,**  **-1e, -1g** |
| **Business Environment** | **ID.BE-5: Resilience requirements to support delivery of critical services are established** | **Third parties must coordinate to ensure that critical services can continue operating in the event of an incident, even under adverse conditions in some instances. For example, alternate communications channels may need to be employed to maintain continuity. Resilience requirements are based on risk assessment and risk management activities.** | * **COBIT 5 DSS04.02** * **ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1** * **NIST SP 800-53 Rev. 4  CP-2, CP-11, SA-14** | **IR-4a, -4b, -4c, -4e** |

|  |  |  |
| --- | --- | --- |
| Protect | Personnel are often the first or second line of defense for the organization’s resources as well as a risk to those assets and resources. Providing access control helps keep assets where they belong. Providing good value to passenger vessel guests includes completion of training requirements and for the protection of resources. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-4, PR.AC-5** | PR.AC-1, PR.AC-2 |
| Awareness and Training | **PR.AT-1, PR.AT-3, PR.AT-5** |  |
| Protective Technology | **PR.PT-1, PR.PT-3** | PR.PT-4 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Access Control | PR.AC-1: Identities and credentials are managed for authorized devices and users | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 16 * COBIT 5 DSS05.04, DSS06.03 * ISA 62443-2-1:2009 4.3.3.5.1 * ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 * ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 * NIST SP 800-53 Rev. 4 AC-2, IA Family | IAM-1a, -1b, -1c, -1d,  -1e, -1f, -1g, RM-1c |
| Access Control | PR.AC-2: Physical access to assets is managed and protected | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS01.04, DSS05.05 * ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 * ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 * NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9 | IAM-2a, -2b, -2c, -2d,  -2e, -2f, -2g |
| **Access Control** | **PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties** | **The concept of separation of duties divides responsibilities and access privileges that together would otherwise enable inappropriate behavior. In smaller organizations, this separation is sometimes challenging and may require additional policy controls to support (e.g., additional account monitoring).**  **The concept of least privilege links authorized accesses to processes, systems, information, and assets directly to job responsibilities. This limits access to those who have a need-to-know and have received proper training for completing their duties.**  **The selection of PR.AC-4 assumes PR.AC-1-3 are being addressed.** | * **CCS CSC 12, 15** * **ISA 62443-2-1:2009 4.3.3.7.3** * **ISA 62443-3-3:2013 SR 2.1** * **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4** * **NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16** | **IAM-2d** |
| **Access Control** | **PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate** | **Control networks each have unique needs and must be managed accordingly. As technologies evolve, more OT systems are being integrated with IT networks for greater ease of activities like management and monitoring, or even convenience of operating a single network. This convergence of IT and OT networks opens new risks to passenger vessel operations. Network integrity is critical to ensuring that OT systems cannot be controlled through IT networks in unanticipated ways. Examples of protecting network integrity include housing OT and IT systems on separate subnets, only allowing one-way flows of information, and blocking outside traffic.** | **ISA 62443-2-1:2009 4.3.3.4**  **ISA 62443-3-3:2013 SR 3.1, SR 3.8**  **ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1**   * **NIST SP 800-53 Rev. 4 AC-4, SC-7** | **CPM-3a, -3b, -3b, -3d** |
| **Awareness and Training** | **PR.AT-1: All users are informed and trained** | **Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related HR roles, responsibilities, and requirements necessary to support passenger vessel operations training accountability. Cybersecurity incidents can impact safety, making training critical for preventing personnel safety impacts.** | * **CCS CSC 9** * **COBIT 5 APO07.03, BAI05.07** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-2, PM-13** | **WM-3a, -4a, -3b, -3c,**  **-3d, -3g, -3h, -3i** |
| **Awareness and Training** | **PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities** | **Cybersecurity incidents can result from mistakes and other unintentional activities, not just malicious actors. Many passenger vessel operations rely heavily on a diverse staff to function. All personnel, regardless of which organization employs them directly, must understand how they may impact cybersecurity and behave accordingly in the context of the specific operations on their vessel.** | * **CCS CSC 9** * **COBIT 5 APO07.03, APO10.04, APO10.05** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 PS-7, SA-9** | **WM-1a, -1b, -1c, -1d,**  **-1e, -1f, -1g** |
| **Awareness and Training** | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in passenger vessel operations must understand the policies and procedures, including role descriptions, that are in place to address cybersecurity risks. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, physical and information security personnel must understand how to prioritize responsibilities as needed.**  **Note that PR.AT-5 assumes implementation of PR.AT-2.** | * **CCS CSC 9** * **COBIT 5 APO07.03** * **ISA 62443-2-1:2009 4.3.2.4.2** * **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** * **NIST SP 800-53 Rev. 4 AT-3, PM-13** | **WM-1a, -1b, -1c, -1d, -1e, -1f, -1g** |
| **Protective Technology** | **PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy** | **Audit/log records are important to verifying the training and other records. The process should follow established records maintenance procedures that document the process and procedures followed. The system implementing the processes and procedures should be regularly reviewed to determine ongoing compliance with policy.** | * **CCS CSC 14** * **COBIT 5 APO11.04** * **ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4** * **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12** * **ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1** * **NIST SP 800-53 Rev. 4 AU Family** | **SA-1a, -1b, -1c, -2a,**  **-2e, -3d, -4e, -4f, -4g** |
| **Protective Technology** | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Provisioning physical and logical access based on the principle of least functionality/privilege limits access to resources to only those who need to access a system or asset and only those assets in the performance of their job duties. Those individuals should be provided adequate training to understand how to properly handle and maintain these assets, thereby limiting access by those who may inadvertently or intentionally cause harm to the assets.** | * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** * **ISO/IEC 27001:2013 A.9.1.2** * **NIST SP 800-53 Rev. 4 AC-3, CM-7** | **IAM-2a, -2b, -2c, -2d,**  **-2e, -2f, -2g, -2h, -2i** |
| Protective Technology | PR.PT-4: Communications and control networks are protected | *Rationale only provided for High Priority Subcategories* | * CCS CSC 7 * COBIT 5 DSS05.02, APO13.01 * ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 * ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 | CPM-3a, -3b, -3c, -3d |

|  |  |  |
| --- | --- | --- |
| Detect | Controls support personnel in meeting their responsibilities. Detection of anomalies and events regarding those controls should be implemented to ensure that they maintain their ability to effectively support guest services and value. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-5** | DE.AE-1 |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Anomalies and Events | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 DSS03.01 * ISA 62443-2-1:2009 4.4.3.3 * NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 | | SA-2a | |
| **Anomalies and Events** | **DE.AE-5: Incident alert thresholds are established** | **Determining incident alert thresholds that support maintaining cyber situational awareness will help ensure that the organization reacts appropriately and in a timely manner when incidents are detected.** | * **COBIT 5 APO12.06** * **ISA 62443-2-1:2009 4.2.3.10** * **NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8** | | **IR-2a, -2d, -2g,**  **TVM-1d, SA-2d, RM-2j** | |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

## **C-8 Mission Objective 8: Maintain Supply Chain and Turnaround**

|  |
| --- |
| ***Mission Objective 8: Maintain Supply Chain and Turnaround***  Managing the movement of personnel, equipment, and supplies that sustain operations, though Access Management, and Risk Management Strategy. Organizations should:   * know which personnel should be where and when, and whether personnel are at the proper location as expected * protect the physical security of personnel, equipment, and supplies from the point of origin to destination * ensure that supplies that support operations are available when needed |

|  |  |  |
| --- | --- | --- |
| Identify | Access and risk management practices define the needs of the passenger vessel operations as they interact with the supply chain during turnaround operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Management | **ID.AM-3, ID.AM-5** | ID.AM-1, ID.AM-6 |
| Risk Management | **ID.RM-3** | ID.RM-1, ID.RM-2 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Asset Management | ID.AM-1: Physical devices and systems within the organization are inventoried | *Rationale only provided for High Priority Subcategories* | * CCS CSC 1 * COBIT 5 BAI09.01, BAI09.02 * ISA 62443-2-1:2009 4.2.3.4 * ISA 62443-3-3:2013 SR 7.8 * ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 * NIST SP 800-53 Rev. 4 CM-8 | ACM-1a, -1c, -1e, -1f |
| **Asset Management** | **ID.AM-3: Organizational communication and data flows are mapped** | **Understanding the flow of data and the communications channels for it is critical to ensuring that the necessary activities are happening when and as intended. In the operational efficiency context, they apply not only to human communications and data flow, but also to communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to performance impacts are identified. Consider frequent communications that are contained on the vessel, external communications, such as those necessary to support GPS navigation, and intermittent or continuous communication and data flow between passenger vessel and onshore facilities.** | * **CCS CSC 1** * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.2.3.4** * **ISO/IEC 27001:2013 A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8** | **RM-2g,**  **AC-1e** |
| **Asset Management** | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Prioritizing resources is a necessary complement to inventory. Potential environmental safety impacts of passenger vessel systems are necessary factors to consider when prioritizing resources. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed, with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |
| Asset Management | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 APO01.02, DSS06.03 * ISA 62443-2-1:2009 4.3.2.3.3 * ISO/IEC 27001:2013 A.6.1.1 * NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 | WM-1a, -1b, -1c |
| Risk Management Strategy | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 * ISA 62443-2-1:2009 4.3.4.2 * NIST SP 800-53 Rev. 4 PM-9 | RM-1a, -1b, -1c, -1d,  -1e, -2a, -2b, -2c, -2d, -2e, 2g, -2h, -2j, -3a,  -3b, -3c, -3d, -3g, -3h,  -3i |
| Risk Management Strategy | ID.RM-2: Organizational risk tolerance is determined and clearly expressed | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 APO12.06 * ISA 62443-2-1:2009 4.3.2.6.5 * NIST SP 800-53 Rev. 4 PM-9 | RM-1c, -1e |
| **Risk Management Strategy** | **ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis** | **Critical infrastructure owners are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient, ultimately supporting our Nation’s success. Protecting the environment is critical to the viability of continued passenger vessel operations. Operations that result in significant harms to the environment will be impeded or even halted, based on the severity of harms.**  **Note that ID.RM-3 assumes implementation of ID.RM-2.** | * **NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14** | **RM-1b, -1c** |

|  |  |  |
| --- | --- | --- |
| Protect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-9 Mission Objective 9: Disembarking, Embarking, and Turnaround**

|  |
| --- |
| ***Mission Objective 9: Disembarking, Embarking, and Turnaround***  Manage the people aspect of port turnaround operations:   * coordinate departure of guests and coordination of their onward journey * coordinate transfer of guest luggage and other items between systems * coordinate arrival of guests and coordinate with their mode of arrival * manage interfaces with all communications with shore and partner systems to provide seamless disembarking and embarking |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management is the primary security category used maintain operational efficiency of passenger vessel operations during disembarking, embarking, and turnaround. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-3, ID.AM-5** | ID.AM-1, ID.AM-6 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Asset Management | ID.AM-1: Physical devices and systems within the organization are inventoried | *Rationale only provided for High Priority Subcategories* | * CCS CSC 1 * COBIT 5 BAI09.01, BAI09.02 * ISA 62443-2-1:2009 4.2.3.4 * ISA 62443-3-3:2013 SR 7.8 * ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 * NIST SP 800-53 Rev. 4 CM-8 | ACM-1a, -1c, -1e, -1f |
| **Asset Management** | **ID.AM-3: Organizational communication and data flows are mapped** | **Understanding the flow of data and the communications channels for it is critical to ensuring that the necessary activities are happening when and as intended. In the operational efficiency context, they apply not only to human communications and data flow, but also to communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to performance impacts are identified. Consider frequent communications that are contained on the vessel, external communications, such as those necessary to support GPS navigation, and intermittent or continuous communication and data flow between passenger vessel and onshore facilities.** | * **CCS CSC 1** * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.2.3.4** * **ISO/IEC 27001:2013 A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8** | **RM-2g,**  **AC-1e** |
| **Asset Management** | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Prioritizing resources is a necessary complement to inventory. Potential environmental safety impacts of passenger vessel systems are necessary factors to consider when prioritizing resources. For example, safety systems are among the highest priority resources, and taking them offline may lead to a failure to identify issues that can impact personnel. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed, with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |
| **Asset Management** | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO01.02, DSS06.03 * ISA 62443-2-1:2009 4.3.2.3.3 * ISO/IEC 27001:2013 A.6.1. * NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 | WM-1a, -1b, -1c |

|  |  |  |
| --- | --- | --- |
| Protect | Access controls and infrastructure protection measures are key protection measures during disembarking, embarking, and turnaround operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-1, PR.AC-2, PR.AC-4** |  |
| Infrastructure Protection | **PR.IP-5, PR.IP-10, PR.IP-11, PR.IP-12** | PR.IP-8 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Access Control** | **PR.AC-1: Identities and credentials are managed for authorized devices and users** | **By ensuring that only authorized users access systems for approved uses, access controls enable stakeholder communications by protecting the devices and information transmitted, addressing important aspects such as need-to-know/confidentiality and ability to log and audit communication streams.** | * **CCS CSC 16** * **COBIT 5 DSS05.04, DSS06.03** * **ISA 62443-2-1:2009 4.3.3.5.1** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9** * **ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3** * **NIST SP 800-53 Rev. 4 AC-2, IA Family** | **IAM-1a, -1b, -1c, -1d,  -1e, -1f, -1g, RM-1c** |
| **Access Control** | **PR.AC-2: Physical access to assets is managed and protected** | **Physical access to passenger vessel operations assets may allow manipulation of those assets in a way that disrupts operations, including disabling an asset and halting operations. Operational harms may range from minor inconvenience to operations to large-scale impacts, and may lead to issues that span other Mission Objectives such as personnel and environmental safety.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8** * **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9** | **IAM-2a, -2b, -2c, -2d,  -2e, -2f, -2g** |
| **Access Control** | **PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties** | **The concept of separation of duties divides responsibilities and access privileges that together would otherwise enable inappropriate behavior. In smaller organizations, this separation is sometimes challenging and may require additional policy controls to support (e.g., additional account monitoring).**  **The concept of least privilege links authorized accesses to processes, systems, information, and assets directly to job responsibilities. This limits access to those who have a need-to-know and have received proper training for completing their duties.**  **The selection of PR.AC-4 assumes PR.AC-1-3 are being addressed.** | * **CCS CSC 12, 15** * **ISA 62443-2-1:2009 4.3.3.7.3** * **ISA 62443-3-3:2013 SR 2.1** * **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4** * **NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16** | **IAM-2d** |
| **Information Protection Processes & Procedures** | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Policies and regulations provide a source of baseline expectations for the operating environment. Deviations in the physical operating environment could be an indication of cyber incidents, making awareness of policy and regulations an important input to cyber situational awareness.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** * **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18** | **ACM-4f,**  **RM-3f** |
| Information Protection Processes & Procedures | PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties | *Rationale only provided for High Priority Subcategories* | * ISO/IEC 27001:2013 A.16.1.6 * NIST SP 800-53 Rev. 4  AC-21, CA-7, SI-4 | ISC 1a, -1b, -1c, -1d,  -1e, -1f, -1g, -1h, -1i,  -1j, -1k, -1l, -2b |
| **Information Protection Processes & Procedures** | **PR.IP-10: Response and recovery plans are tested** | **Periodically testing response and recovery plans for passenger vessel operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization’s chances of restoring operational security efficiently and effectively.** | * **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** * **ISA 62443-3-3:2013 SR 3.3** * **ISO/IEC 27001:2013 A.17.1.3**   **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14** | **IR-3e, -4f, -3k, -4i, -4j** |
| **Information Protection Processes & Procedures** | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Passenger vessel operations rely on personnel to operate and maintain assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right assets at the right times, through activities such as screening personnel against applicable safety and knowledge conditions, provisioning and deprovisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.** | * **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** * **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** * **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** * **NIST SP 800-53 Rev. 4 PS Family** | **WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |
| **Information Protection Processes & Procedures** | **PR.IP-12: A vulnerability management plan is developed and implemented** | **Passenger vessel operations must account for a number of system vulnerabilities. It is important to have supplemental security controls to protect these vulnerabilities both at steady state and when attempts at compromise are recognized. To prepare for this a vulnerability management plan should be developed, implemented, tested, and maintained** | * **ISO/IEC 27001:2013 A.12.6.1, A.18.2.2** * **NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2** | **TVM-3a, -3e** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | **N/A** | N/A |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| N/A | N/A | N/A | N/A | | N/A | |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

## **C-10 Mission Objective 10: Coordinate Port Operations**

|  |
| --- |
| ***Mission Objective 10: Coordinate Port Operations***  Manage the ship and supply coordination of Port Operations:   * coordinate port arrival and departure regulations, procedures, and protocols * coordinate incoming food and other perishable supplies * coordinate resupply of fuel * coordinate sewage offload |

|  |  |  |
| --- | --- | --- |
| Identify | Good understanding of risks to the business environment are key categories as passenger vessels coordinate port operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-1, ID.BE-4, ID.BE-5** | ID.BE-2, ID.BE-3 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Business Environment** | **ID.BE-1: The organization’s role in the supply chain is identified and communicated** | **Mission-critical functions can reside in many places within passenger vessel operations supply chain. Understanding which processes, systems, and assets are most critical allows traceability from critical business and mission systems to system hardware, software, and firmware components. Knowing which aspects of passenger vessel operations are most critical also helps organizations identify their specific role(s) in the supply chain and tailor their activities accordingly.** | * **COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05** * **ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2** * **NIST SP 800-53 Rev. 4  CP-2, SA-12** | **EDM-1b, -1d, -1f, -1g**  **RM-1c** |
| Business Environment | ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated | ***Rationale only provided for High Priority Subcategories*** | * **COBIT 5 APO02.06, APO03.01** * **NIST SP 800-53 Rev. 4 PM-8** | **EDM-1b, -1c, -1d, -1f, -1g** |
| Business Environment | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO02.01, APO02.06, APO03.01 * ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 * NIST SP 800-53 Rev. 4 PM-11, SA-14 | RM-3b, -1c |
| **Business Environment** | **ID.BE-4: Dependencies and critical functions for delivery of critical services are established** | **Dependency and criticality analysis informs protection activities that are critical to maintaining the passenger vessel operations activities required for operational efficiency. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated operational functions and activities, as well as traceability to specific assets.** | * **ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3** * **NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14** | **ACM-1a, -1b, -1c, -1d, -1e, -1f,**  **EDM-1a, -1c,**  **-1e, -1g** |
| **Business Environment** | **ID.BE-5: Resilience requirements to support delivery of critical services are established** | **Third parties must coordinate to ensure that critical services can continue operating in the event of an incident, even under adverse conditions in some instances. For example, alternate communications channels may need to be employed to maintain continuity. Resilience requirements are based on risk assessment and risk management activities.** | * **COBIT 5 DSS04.02** * **ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1** * **NIST SP 800-53 Rev. 4  CP-2, CP-11, SA-14** | **IR-4a, -4b, -4c, -4e** |

|  |  |  |
| --- | --- | --- |
| Protect | Access controls and protection procedures and processesare key to protecting passenger vessels during the coordination of port operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-2, PR.AC-4, PR.AC-5** |  |
| Information Protection Processes and Procedures | **PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-9, PR.IP-10, PR.IP-11, PR.IP-12** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Access Control** | **PR.AC-2: Physical access to assets is managed and protected** | **Physical access to passenger vessel operations assets may allow manipulation of those assets in a way that disrupts operations, including disabling an asset and halting operations. Operational harms may range from minor inconvenience to operations to large-scale impacts, and may lead to issues that span other Mission Objectives, such as personnel and environmental safety.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8** * **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9** | **IAM-2a, -2b, -2c, -2d,  -2e, -2f, -2g** |
| **Access Control** | **PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties** | **The concept of separation of duties divides responsibilities and access privileges that together would otherwise enable inappropriate behavior. In smaller organizations, this separation is sometimes challenging and may require additional policy controls to support (e.g., additional account monitoring).**  **The concept of least privilege links authorized accesses to processes, systems, information, and assets directly to job responsibilities. This limits access to those who need to know and have received proper training for completing their duties.**  **The selection of PR.AC-4 assumes PR.AC-1-3 are being addressed.** | * **CCS CSC 12, 15** * **ISA 62443-2-1:2009 4.3.3.7.3** * **ISA 62443-3-3:2013 SR 2.1** * **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4** * **NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16** | **IAM-2d** |
| **Access Control** | **PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate** | **IT and OT/process control networks each have unique needs and must be managed accordingly. As technologies evolve, more OT systems are being integrated with IT networks for greater ease of activities like management and monitoring, or even convenience of operating a single network. This convergence of IT and OT networks opens new risks to passenger vessel operations. Network integrity is critical to ensuring that OT systems cannot be controlled through IT networks in unanticipated ways. Examples of protecting network integrity include housing OT and IT systems on separate subnets, only allowing one-way flows of information, and blocking outside traffic.** | * **ISA 62443-2-1:2009 4.3.3.4** * **ISA 62443-3-3:2013 SR 3.1, SR 3.8** * **ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, SC-7** | **CPM-3a, -3b, -3b, -3d** |
| **Information Protection Processes & Procedures** | **PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained** | **Validated and tested baseline configurations promote consistency when configuring new systems and provide a reliable operating state. Baselines also support response and recovery efforts in returning to a reliable operating state after an incident. Organizations that need help getting started with baselines may choose to use available resources from security researchers, trade associations, standards bodies, and others, augmenting and tailoring those resources over time as they learn about their environment’s unique needs.** | * **CCS CSC 3, 10** * **COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** | **ACM-2a, -2b, -2c, -2d, -2e** |
| **Information Protection Processes & Procedures** | **PR.IP-3: Configuration change control processes are in place** | **Change control processes provide a structured approach to managing changes to existing systems, ensuring that each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports reliability by limiting the potential for unplanned changes and managing planned changes in accordance with decisions previously made, as well as vetted organizational requirements and standards to limit adverse impacts.** | * **COBIT 5 BAI06.01, BAI01.06** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10** | **ACM-3a, -3b, -3c, -3d,**  **-3e, -3f, -4a, -4e** |
| **Information Protection Processes and Procedures** | **PR.IP-4: Backups of information are conducted, maintained, and tested periodically** | **When cybersecurity incidents occur, good backups are one of the things that enable organizations to expediently return to a desirable state. Information backed up may also include user-level and system-level information. The confidentiality, integrity, and availability of backup media should be well protected to ensure that quality backups are available when needed. Testing should be periodically conducted to ensure that the technology is still available and usable to access the backup information and systems.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.9** * **ISA 62443-3-3:2013 SR 7.3, SR 7.4** * **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3** * **NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9** | **IR-4a, -4b** |
| **Information Protection Processes & Procedures** | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Policies and regulations provide a source of baseline expectations for the operating environment. Deviations in the physical operating environment could be an indication of cyber incidents, making awareness of policy and regulations an important input to cyber situational awareness.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** * **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18** | **ACM-4f,**  **RM-3f** |
| **Information Protection Processes & Procedures** | **PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed** | **Passenger vessel operations response and recovery plans define the degree of IT and OT operations necessary to return to a desired minimum state of operations after a cybersecurity event. Developing and managing these plans in coordination with incident response processes ensures that the necessary activities occur when a cybersecurity event is identified. Instituting processes to manage response and recovery plans ensures that they are periodically updated, allowing the organization to maintain an acceptable level of preparedness. This activity supports response and recovery activities so that passenger vessel operations can return to a desirable state expediently.**  **Note that PR.IP-9 assumes PR.IP-10 is addressed. Note also, PR.IP-9 and PR.IP-12 should be developed and maintained with coordination.** | * **COBIT 5 DSS04.03** * **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** * **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2** * **NIST SP 800-53 Rev. 4 CP-2, IR-8** | **IR-3f, 3k, -3m, 4c, -4d, -4f, -4i, 4j, -5a, -5b,**  **-5c, -5e, -5f, -5g, -5h,**  **-5i,**  **TVM-1d,**  **RM-1c** |
| **Information Protection Processes & Procedures** | **PR.IP-10: Response and recovery plans are tested** | **Periodically testing response and recovery plans for passenger vessel operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization’s chances of restoring operational security efficiently and effectively.** | * **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** * **ISA 62443-3-3:2013 SR 3.3** * **ISO/IEC 27001:2013 A.17.1.3** * **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14** | **IR-3e, -4f, -3k, -4i, -4j** |
| **Information Protection Processes & Procedures** | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Passenger vessel operations rely on personnel to operate and maintain IT and OT assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right assets at the right times, through activities such as screening personnel against applicable safety and knowledge conditions, provisioning and deprovisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.** | * **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** * **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** * **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** * **NIST SP 800-53 Rev. 4 PS Family** | **WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |
| **Information Protection Processes & Procedures** | **PR.IP-12: A vulnerability management plan is developed and implemented** | **Passenger vessel operations must account for a number of system vulnerabilities. It is important to have supplemental security controls to protect these vulnerabilities both at steady state and when attempts at compromise are recognized. To prepare for this, a vulnerability management plan should be developed, implemented, tested, and maintained.** | * **ISO/IEC 27001:2013 A.12.6.1, A.18.2.2** * **NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2** | **TVM-3a, -3e** |

|  |  |  |
| --- | --- | --- |
| Detect | Detecting anomalies and events quickly is key to passenger vessels as they coordinate port operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-4, DE.AE-5** | DE.AE-2 |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Anomalies and Events | DE.AE-2: Detected events are analyzed to understand attack targets and methods | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 * ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 * ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI4 | | IR-1f, -2l, 3h | |
| **Anomalies and Events** | **DE.AE-4: Impact of events is determined** | **Knowing the impact of events helps organizations understand the impact to maintaining the integrity and continuity of passenger vessel operations, how to appropriately respond, and what measures may be necessary to recover from the event.** | * **COBIT 5 APO12.06** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4** | | **IR-2b, -2d, -2g,**  **TVM-1d,**  **RM-2j** | |
| **Anomalies and Events** | **DE.AE-5: Incident alert thresholds are established** | **Determining incident alert thresholds that support maintaining cyber situational awareness will help ensure that the organization reacts appropriately and in a timely manner when incidents are detected.** | * **COBIT 5 APO12.06** * **ISA 62443-2-1:2009 4.2.3.10** * **NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8** | **IR-2a, -2d, -2g,**  **TVM-1d, SA-2d, RM-2j** | |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | **N/A** | **N/A** |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | **N/A** | **N/A** | **N/A** | **N/A** |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | **N/A** | **N/A** |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | **N/A** | **N/A** | **N/A** | **N/A** |

## **C-11 Mission Objective 11: Assure (Optimize) Asset Lifecycle Management**

|  |
| --- |
| ***Mission Objective 11: Assure (Optimize) Asset Lifecycle Management***  Manage and optimize the operational uptime of all capabilities:   * coordinate maintenance and repair to minimize disruption * assure ready spares and systems/process redundancy to assure availability * manage assets to track effective useable life, end-of-life swap-out, systems replacement and upgrades |

|  |  |  |
| --- | --- | --- |
| Identify | Proper asset management and understanding the security risks in the business environment is key to proper assurance and optimization of assets during the full lifecycle of passenger vessel operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-5** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Asset Management** | **ID.AM-1: Physical devices and systems within the organization are inventoried** | **Maintaining a current inventory of the physical devices and systems that support passenger vessel operations provides the foundation for identifying and prioritizing assets that are most critical to maintaining the continuity and integrity of operations.** | * **CCS CSC 1** * **COBIT 5 BAI09.01, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.4** * **ISA 62443-3-3:2013 SR 7.8** * **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** * **NIST SP 800-53 Rev. 4 CM-8** | **ACM-1a, -1c, -1e, -1f** |
| **Asset Management** | **ID.AM-2: Software platforms and applications within the organization are inventoried** | **Understanding the inventory of software platforms and applications that support passenger vessel operations is critical to ensuring that vessel software is properly understood, supported, and maintained, as well as providing adequate visibility into operations.** | * **CCS CSC 2** * **COBIT 5 BAI09.01, BAI09.02, BAI09.05** * **ISA 62443-2-1:2009 4.2.3.4** * **ISA 62443-3-3:2013 SR 7.8** * **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** * **NIST SP 800-53 Rev. 4 CM-8** | **ACM-1a, -1c, -1e, -1f** |
| Asset Management | **ID.AM-3: Organizational communication and data flows are mapped** | **Understanding the flow of data and the communications channels for it is critical to ensuring that the necessary activities are happening when and as intended. In the operational efficiency context, they apply not only to human communications and data flow, but also to communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to performance impacts are identified. Consider frequent communications that are contained on the vessel, external communications, such as those necessary to support GPS navigation, and intermittent or continuous communication and data flow between passenger vessel and onshore facilities.** | * **CCS CSC 1** * **COBIT 5 DSS05.02** * **ISA 62443-2-1:2009 4.2.3.4** * **ISO/IEC 27001:2013 A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8** | **RM-2g,**  **AC-1e** |
| **Asset Management** | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Prioritizing resources is a necessary complement to inventory. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed, with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful. Also, potential environmental safety impacts of passenger vessel systems are necessary factors to consider when prioritizing resources. For example, safety systems are among the highest priority resources, and taking them offline may lead to a failure to identify issues that can impact personnel.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02** * **ISA 62443-2-1:2009 4.2.3.6** * **ISO/IEC 27001:2013 A.8.2.1** * **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14** | **ACM-1a, -1b, -1c, -1d** |

|  |  |  |
| --- | --- | --- |
| Protect | Maintenance is a key category when assuring and optimizing asset management for the full lifecycle of passenger vessel operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Maintenance | **PR.MA-1, PR.MA-2** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Maintenance** | **PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools** | **Properly maintaining passenger vessel assets safeguards against preventable issues that could impact readiness and regulatory compliance. Managing maintenance through a defined approval process and with controlled tools protects the organization from introducing unnecessary risks, such as performing maintenance during a time that impacts other assets, changing implemented controls in a way that renders them ineffective, running tools that have not been scanned for malicious activity, or allowing access to unescorted and/or unauthorized individuals. For some assets, the ability to operate requires review and/or authorization and maintenance regimes by government regulators, standards bodies, or class societies.** | * **COBIT 5 BAI09.03** * **ISA 62443-2-1:2009 4.3.3.3.7** * **ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5** * **NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5** | **ACM-3b, -4c, -3f** |
| **Maintenance** | **PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access** | **Remote maintenance requires supplemental processes to support it. While all maintenance should be conducted through a defined approval process and with controlled tools to protect the organization from introducing unnecessary risks, some maintenance must be conducted through remote processes.**  **Whether direct or remote, maintenance should avoid and detect if it implements controls in a way that renders them ineffective for other processes or mission objectives, running tools that have not been scanned for malicious activity, or allowing access to unauthorized individuals or supply chain partners.**  **For some assets, the ability to operate requires review and/or authorization and maintenance regimes by government regulators, standards bodies, or class societies.** | * **COBIT 5 DSS05.04** * **ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8** * **ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1** * **NIST SP 800-53 Rev. 4 MA-4** | **SA-1a,**  **IR-1C,**  **IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | **N/A** | **N/A** |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

## **C-12 Mission Objective 12: Maintain Passenger Information and Accounting Systems**

|  |
| --- |
| ***Mission Objective 12: Maintain Passenger Information and Accounting Systems***  Recognize cybersecurity role in the passenger back office systems:   * provide security to non-customer-facing IT * manage support systems security * identify and securely protect guest personally identifiable information (PII) * manage interfaces and data shared with business partners |

|  |  |  |
| --- | --- | --- |
| Identify | N/A | |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

| Protect | Access controls and adequate data security are key control categories for maintaining passenger information and accounting systems. | |
| --- | --- | --- |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-1, PR.AC-4, PR.AC-5** |  |
| Data Security | **PR.DS-1, PR.DS-2, PR.DS-5** | PR.DS-4, PR-DS-6 |
| Information Protection Processes & Procedures | **PR.IP-1, PR.IP-3, PR-IP-4, PR.IP-5, PR.IP-10, PR.IP-11** | PR.IP-6, PR.IP-7 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Access Control** | **PR.AC-1: Identities and credentials are managed for authorized devices and users** | **By ensuring that only authorized users access systems for approved uses, access controls enable stakeholder communications by protecting the devices and information transmitted, addressing important aspects such as need-to-know/confidentiality and ability to log and audit communication streams.** | * **CCS CSC 16** * **COBIT 5 DSS05.04, DSS06.03** * **ISA 62443-2-1:2009 4.3.3.5.1** * **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9** * **ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3** * **NIST SP 800-53 Rev. 4 AC-2, IA Family** | **IAM-1a, -1b, -1c, -1d,  -1e, -1f, -1g, RM-1c** |
| **Access Control** | **PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties** | **The concept of separation of duties divides responsibilities and access privileges that together would otherwise enable inappropriate behavior. In smaller organizations, this separation is sometimes challenging and may require additional policy controls to support (e.g., additional account monitoring).**  **The concept of least privilege links authorized access to processes, systems, information, and assets directly to job responsibilities. This limits access to those who need to know and have received proper training for completing their duties.**  **The selection of PR.AC-4 assumes PR.AC-1-3 are being addressed.** | * **CCS CSC 12, 15** * **ISA 62443-2-1:2009 4.3.3.7.3** * **ISA 62443-3-3:2013 SR 2.1** * **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4** * **NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16** | **IAM-2d** |
| **Access Control** | **PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate** | **Network integrity is critical to ensuring that IT systems cannot be controlled in unanticipated ways. Examples of protecting network integrity include housing OT and IT systems on separate subnets, only allowing one-way flows of information, and blocking outside traffic.** | **ISA 62443-2-1:2009 4.3.3.4**  **ISA 62443-3-3:2013 SR 3.1, SR 3.8**  **ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1**   * **NIST SP 800-53 Rev. 4 AC-4, SC-7** | **CPM-3a, -3b, -3b, -3d** |
| **Data Security** | **PR.DS-1: Data-at-rest is protected** | **Communications data resides on storage devices for some period of time. For example, configuration settings are stored on network devices. This type of data should be protected locally where it is stored. Protection techniques may also include encryption and offline storage when additional protections are needed.** | * **CCS CSC 17** * **COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06** * **ISA 62443-3-3:2013 SR 3.4, SR 4.1** * **ISO/IEC 27001:2013 A.8.2.3** * **NIST SP 800-53 Rev. 4 SC-28** | **TVM-1c, -2c** |
| **Data Security** | **PR.DS-2: Data-in-transit is protected** | **Data must be protected as it travels across internal and external networks, particularly external networks where it may be subject to interception or modification.** | * **CCS CSC 17** * **COBIT 5 APO01.06, DSS06.06** * **ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2** * **ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3** * **NIST SP 800-53 Rev. 4 SC-8** | **TVM-1c, -2c** |
| Data Security | PR.DS-4: Adequate capacity to ensure availability is maintained | *Rationale only provided for High Priority Subcategories* | * **COBIT 5 APO13.01** * **ISA 62443-3-3:2013 SR 7.1, SR 7.2** * **ISO/IEC 27001:2013 A.12.3.1** * **NIST SP 800-53 Rev. 4  AU-4, CP-2, SC-5** | **TVM-1c, -2c**  **CPM-**3b |
| **Data Security** | **PR.DS-5: Protections against data leaks are implemented** | **Communications can relay valuable information about the health of data activities, proprietary and safety information about instructions for handling incidents, and other sensitive information. Leaks of this information could range in impact due to a loss of control of the information.**  **Security categories or classifications of information influence the level of protections implemented to protect the communications channels and the information that flows across them.** | * **CCS CSC 17** * **COBIT 5 APO01.06** * **ISA 62443-3-3:2013 SR 5.2** * **ISO/IEC 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** * **NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4** | **CPM-3b**  **TVM-1c, -2c, -2n** |
| Data Security | PR.DS-6 | *Rationale only provided for High Priority Subcategories* | * **ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8** * **ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3** * **NIST SP 800-53 Rev. 4 SI-7** | **SA-2e, -2i** |
| **Information Protection Processes & Procedures** | **PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained** | **Validated and tested baseline configurations promote consistency when configuring new systems and provide a reliable operating state. Baselines also support response and recovery efforts in returning to a reliable operating state after an incident. Organizations that need help getting started with baselines may choose to use available resources from security researchers, trade associations, standards bodies, and others, augmenting and tailoring those resources over time as they learn about their environment’s unique needs.** | * **CCS CSC 3, 10** * **COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** | **ACM-2a, -2b, -2c, -2d, -2e** |
| **Information Protection Processes & Procedures** | **PR.IP-3: Configuration change control processes are in place** | **Change control processes provide a structured approach to managing changes to existing systems, ensuring that each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports reliability by limiting the potential for unplanned changes and managing planned changes in accordance with decisions previously made, as well as vetted organizational requirements and standards to limit adverse impacts.** | * **COBIT 5 BAI06.01, BAI01.06** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10** | **ACM-3a, -3b, -3c, -3d, -4a, -3e, -3f, -4e** |
| **Information Protection Processes and Procedures** | **PR.IP-4: Backups of information are conducted, maintained, and tested periodically** | **When cybersecurity incidents occur, good backups are one of the things that enable organizations to expediently return to a desirable state. Information backed up may also include user-level and system-level information. The confidentiality, integrity, and availability of backup media should be well protected to ensure that quality backups are available when needed. Testing should be periodically conducted to ensure that the technology is still available and usable to access the backup information and systems.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.9** * **ISA 62443-3-3:2013 SR 7.3, SR 7.4** * **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3** * **NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9** | **IR-4a, -4b** |
| **Information Protection Processes & Procedures** | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Policies and regulations provide a source of baseline expectations for the operating environment. Deviations in the physical operating environment could be an indication of cyber incidents, making awareness of policy and regulations an important input to cyber situational awareness.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** * **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18** | **ACM-4f,**  **RM-3f** |
| Information Protection Processes & Procedures | PR.IP-6: Data is destroyed according to policy | *Rationale only provided for High Priority Subcategories* | * COBIT 5 BAI09.03 * ISA 62443-2-1:2009 4.3.4.4 * ISA 62443-3-3:2013 SR 4.2 * ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A 11.2.7 * NIST SP 800-53 Rev. 4 MP-6 | ACM-3d |
| Information Protection Processes & Procedures | PR.IP-7: Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1: 2009 .4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 * NIST 800.53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 | CPM-1g |
| **Information Protection Processes & Procedures** | **PR.IP-10: Response and recovery plans are tested** | **Periodically testing response and recovery plans for passenger vessel operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization’s chances of restoring operational security efficiently and effectively.** | * **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** * **ISA 62443-3-3:2013 SR 3.3** * **ISO/IEC 27001:2013 A.17.1.3** * **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14** | **IR-3e, -4f, -3k, -4i, -4j** |
| **Information Protection Processes & Procedures** | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Passenger vessel operations rely on personnel to operate and maintain assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right assets at the right times, through activities such as screening personnel against applicable safety and knowledge conditions, provisioning and deprovisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.** | * **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** * **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** * **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** * **NIST SP 800-53 Rev. 4 PS Family** | **WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

## **C-13 Mission Objective 13: Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology**

|  |
| --- |
| ***Mission Objective 13: Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology***  Recognize cybersecurity effects on the back-office operations. Prevent harm to systems and services infrastructure:   * manage risk to all back-office systems * maintain account management security * manage support systems security * identify and securely protect guest personally identifiable information (PII) * control interfaces and data shared with business partners |

|  |  |  |
| --- | --- | --- |
| Identify | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|  | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Protect | Adequate awareness and training, data security activities, protection processes and procedures as well as protective technologies all make up the suite of protection categories required to manage, monitor and maintain non-guest-facing back office technology for passenger vessel operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-4, PR.AC-5** |  |
| Data Security | **PR.DS-1, PR.DS-2, PR.DS-5** | PR.DS-4, PR.DS-6 |
| Information Protection Processes & Procedures | **PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-10, PR.IP-11** | PR.IP-6, PR.IP-7 |
| Protective Technologies | **PR.PT-1, PR.PT-4** | PR.PT-3 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **Access Control** | **PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties** | **The concept of separation of duties divides responsibilities and access privileges that together would otherwise enable inappropriate behavior. In smaller organizations, this separation is sometimes challenging and may require additional policy controls to support (e.g., additional account monitoring).**  **The concept of least privilege links authorized accesses to processes, systems, information, and assets directly to job responsibilities. This limits access to those who need to know and have received proper training for completing their duties.**  **The selection of PR.AC-4 assumes PR.AC-1-3 is being addressed.** | * **CCS CSC 12, 15** * **ISA 62443-2-1:2009 4.3.3.7.3** * **ISA 62443-3-3:2013 SR 2.1** * **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4** * **NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16** | **IAM-2d** |
| **Access Control** | **PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate** | **Process control networks each have unique needs and must be managed accordingly. Network integrity is critical to ensuring that systems cannot be controlled through IT networks in unanticipated ways. Examples of protecting network integrity includes housing systems on separate subnets, only allowing one-way flows of information, and blocking outside traffic.** | **ISA 62443-2-1:2009 4.3.3.4**  **ISA 62443-3-3:2013 SR 3.1, SR 3.8**  **ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1**   * **NIST SP 800-53 Rev. 4 AC-4, SC-7** | **CPM-3a, -3b, -3b, -3d** |
| **Data Security** | **PR.DS-1: Data-at-rest is protected** | **Communications data resides on storages devices for some period of time. For example, configuration settings are stored on network devices. This type of data should be protected locally where it is stored. Protection techniques may also include encryption and offline storage when additional protections are needed.** | * **CCS CSC 17** * **COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06** * **ISA 62443-3-3:2013 SR 3.4, SR 4.1** * **ISO/IEC 27001:2013 A.8.2.3** * **NIST SP 800-53 Rev. 4 SC-28** | **TVM-1c, -2c** |
| **Data Security** | **PR.DS-2: Data-in-transit is protected** | **IT and OT data must be protected as it travels across internal and external networks, particularly external networks where it may be subject to interception or modification.** | * **CCS CSC 17** * **COBIT 5 APO01.06, DSS06.06** * **ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2** * **ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3** * **NIST SP 800-53 Rev. 4 SC-8** | **TVM-1c, -2c** |
| Data Security | PR.DS-4: Adequate capacity to ensure availability is maintained | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01 * ISA 62443-3-3:2013 SR 7.1, SR 7.2 * ISO/IEC 27001:2013 A.12.3.1 * NIST SP 800-53 Rev. 4  AU-4, CP-2, SC-5 | TVM-1c, -2c  CPM-3b |
| **Data Security** | **PR.DS-5: Protections against data leaks are implemented** | **Communications can relay valuable information about the health of IT and OT activities, proprietary and safety information about instructions for handling incidents, and other sensitive information. Leaks of this information could range in impact due to a loss of control of the information.**  **Security categories or classifications of information influence the level of protections implemented to protect the communications channels and the information that flows across them.** | * **CCS CSC 17** * **COBIT 5 APO01.06** * **ISA 62443-3-3:2013 SR 5.2** * **ISO/IEC 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** * **NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4** | **CPM-3b**  **TVM-1c, -2c, -2n** |
| Data Security | PR.DS-6 | *Rationale only provided for High Priority Subcategories* | * ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 * ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 * NIST SP 800-53 Rev. 4 SI-7 | SA-2e, -2i |
| **Information Protection Processes & Procedures** | **PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained** | **Validated and tested baseline configurations promote consistency when configuring new systems and provide a reliable operating state. Baselines also support response and recovery efforts in returning to a reliable operating state after an incident. Organizations that need help getting started with baselines may choose to use available resources from security researchers, trade associations, standards bodies, and others, augmenting and tailoring those resources over time as they learn about their environment’s unique needs.** | * **CCS CSC 3, 10** * **COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10** | **ACM-2a, -2b, -2c, -2d, -2e** |
| **Information Protection Processes & Procedures** | **PR.IP-3: Configuration change control processes are in place** | **Change control processes provide a structured approach to managing changes to existing systems, ensuring that each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports reliability by limiting the potential for unplanned changes and managing planned changes in accordance with decisions previously made, as well as vetted organizational requirements and standards to limit adverse impacts.** | * **COBIT 5 BAI06.01, BAI01.06** * **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** * **ISA 62443-3-3:2013 SR 7.6** * **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** * **NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10** | **ACM-3a, -3b, -3c, -3d, -4a, -3e, -3f, -4e** |
| **Information Protection Processes and Procedures** | **PR.IP-4: Backups of information are conducted, maintained, and tested periodically** | **When cybersecurity incidents occur, good backups are one of the things that enable organizations to expediently return to a desirable state. Information backed up may also include user-level and system-level information. The confidentiality, integrity, and availability of backup media should be well protected to ensure that quality backups are available when needed. Testing should be periodically conducted to ensure that the technology is still available and usable to access the backup information and systems.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.9** * **ISA 62443-3-3:2013 SR 7.3, SR 7.4** * **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3** * **NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9** | **IR-4a, -4b** |
| **Information Protection Processes & Procedures** | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Policies and regulations provide a source of baseline expectations for the operating environment. Deviations in the physical operating environment could be an indication of cyber incidents, making awareness of policy and regulations an important input to cyber situational awareness.** | * **COBIT 5 DSS01.04, DSS05.05** * **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** * **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** * **NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18** | **ACM-4f,**  **RM-3f** |
| Information Protection Processes & Procedures | PR.IP-6: Data is destroyed according to policy | *Rationale only provided for High Priority Subcategories* | * COBIT 5BAI09.03 * ISA 62443-2-1:2009 4.3.4.4 * ISA 62443-3-3:2013 SR 4.2 * ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A 11.2.7 * NIST SP 800-53 Rev. 4 MP-6 | ACM-3d |
| Information Protection Processes & Procedures | PR.IP-7**:** Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1: 2009 .4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 * NIST 800.53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 | CPM-1g |
| **Information Protection Processes & Procedures** | **PR.IP-10: Response and recovery plans are tested** | **Periodically testing response and recovery plans for passenger vessel operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization’s chances of restoring operational security efficiently and effectively.** | * **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** * **ISA 62443-3-3:2013 SR 3.3** * **ISO/IEC 27001:2013 A.17.1.3** * **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14** | **IR-3e, -4f, -3k, -4i, -4j** |
| **Information Protection Processes & Procedures** | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Passenger vessel operations rely on personnel to operate and maintain assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right assets at the right times, through activities such as screening personnel against applicable safety and knowledge conditions, provisioning and deprovisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.** | * **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** * **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** * **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** * **NIST SP 800-53 Rev. 4 PS Family** | **WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |
| **Protective Technology** | **PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy** | **Audit/log records are important to verifying the training and other records. The process should follow established records maintenance procedures that document the process and procedures followed. The system implementing the processes and procedures should be regularly reviewed to determine ongoing compliance with policy.** | * **CCS CSC 14** * **COBIT 5 APO11.04** * **ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4** * **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12** * **ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1** * **NIST SP 800-53 Rev. 4 AU Family** | **SA-1a, -1b, -1c, -2a,**  **-2e, -3d, -4e, -4f, -4g** |
| Protective Technology | PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.02 * ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 * ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 * ISO/IEC 27001:2013 A.9.1.2 * NIST SP 800-53 Rev. 4 AC-3, CM-7 | IAM-2a, -2b, -2c, -2d,  -2e, -2f, -2g, -2h, -2i |
| **Protective Technology** | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to passenger vessel assets. For example, information about OT assets may be sent to an onshore facility for monitoring. This access can provide useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in operational security issues.** | * **CCS CSC 7** * **COBIT 5 DSS05.02, APO13.01** * **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** * **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** * **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7** | **CPM-3a, -3b, -3c, -3d** |

|  |  |  |
| --- | --- | --- |
| Detect | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| N/A | **N/A** | **N/A** |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| N/A | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Respond | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| Recover | N/A | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| **N/A** | N/A | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| **N/A** | N/A | N/A | N/A | N/A |

1. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, “Risk Response Strategies” [↑](#footnote-ref-1)
2. NIST has conducted extensive research regarding risk management practices. FIPS 199, while merely informative for the purposes of these Mission Objectives, defines levels of risk in terms of low, moderate, and high that may provide useful delineations in some contexts. [↑](#footnote-ref-2)
3. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, “Risk Response Strategies” [↑](#footnote-ref-3)
4. NIST has conducted extensive research regarding risk management practices. FIPS 199, while merely informative for the purposes of these Mission Objectives, defines levels of risk in terms of low, moderate, and high that may provide useful delineations in some contexts. [↑](#footnote-ref-4)