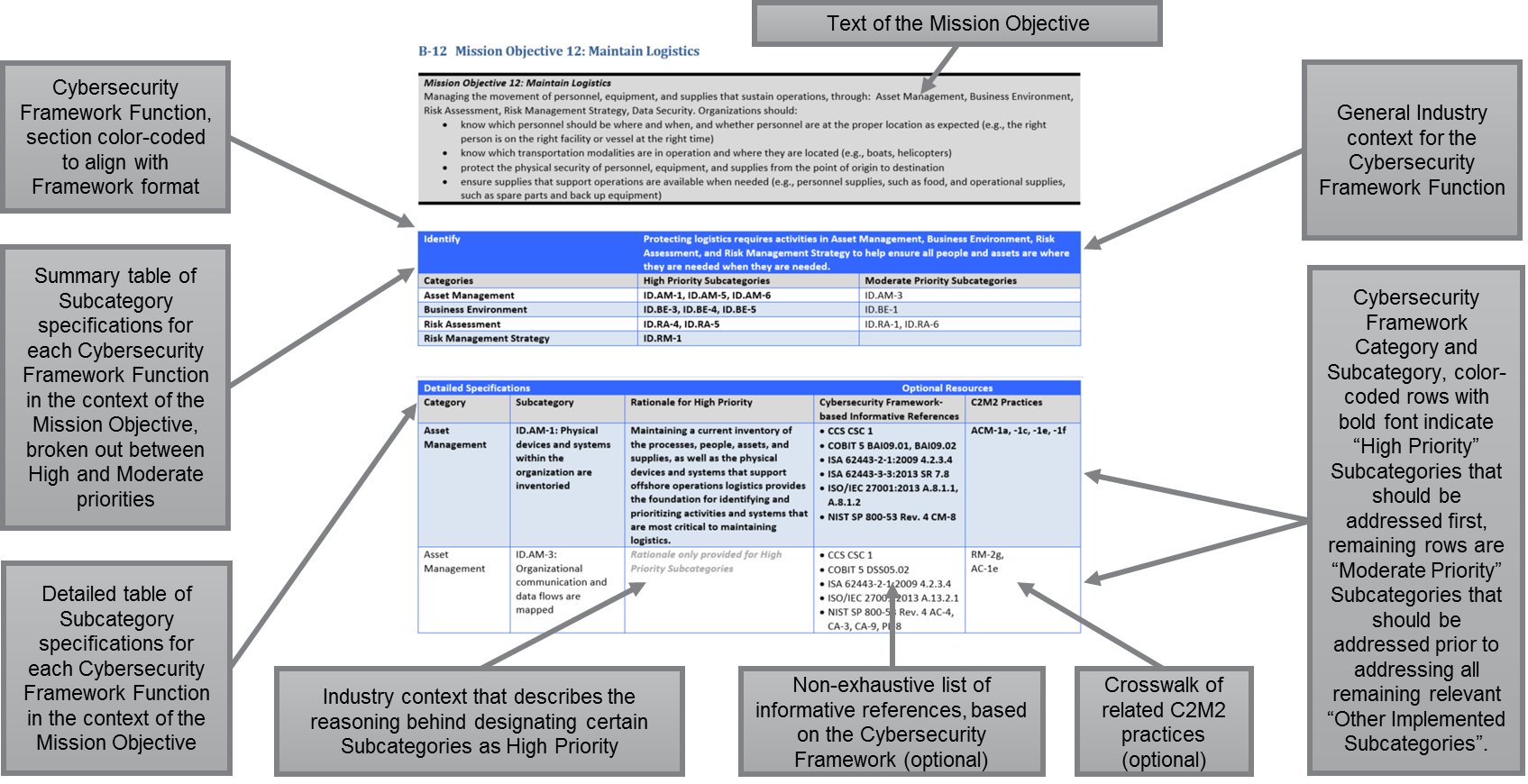
# Offshore Operations Profile

This Offshore Operations CFP defines the desired minimum state of cybersecurity by identifying the minimum set of Cybersecurity Framework Categories and Subcategories for each of the twelve Mission Objectives required to conduct Offshore Operations in a more secure manner. Appendix B is divided into a subsection for each of the twelve Mission Objectives listed in Section 6.3, Table 6-3 of the profile overview document. Each Mission Objective subsection in Appendix B includes both a summary and detailed table of High and Moderate Priority Subcategory specifications in the Profile by Cybersecurity Framework Function and Category. Figure B-1 provides a legend that describes the layout of the detailed Profile content provided.

Figure B‑1. Appendix B Content Legend



## **B-1 Mission Objective 1: Maintain Personnel Safety**

|  |
| --- |
| ***Mission Objective 1: Maintain Personnel Safety***  Recognizing cybersecurity-effects on process control systems that impact personnel safety. Preventing injury, including loss of life through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. Organizations should:   * account for all personnel on board offshore facilities and vessels * understand scope of operational threats and their potential adverse 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 | Asset management, risk assessment and risk management processes are the primary method used to identify procedures, technologies, and equipment that may impact the organization’s ability to maintain personnel safety. Each organization’s approach to implementing the Cybersecurity Framework Core is based on the decisions made as a result of risk assessments. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID-AM-1, ID.AM-2, ID.AM-3, ID.AM-5, ID.AM-6** | ID.AM-4 |
| Risk Assessment | **ID.RA-5,** **ID.RA-6** | ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4 |
| Risk Management Strategy | **ID.RM-1, ID.RM-3** |  |

| 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 offshore operations is a foundational activity that supports:**   * **identifying and prioritizing assets that have personnel safety impacts** * **recognizing specific equipment that is being effected and effectively responding during an incident** * **understanding gaps in redundancy and failover (Response Subcategories become more important without adequate redundancy and failover)**     **This Subcategory should also be extended to account for personnel assets. Understanding which personnel are present on a vessel or facility at any given time is critical for determining who may be impacted by the physical effects of a cybersecurity incident.**  **With physical impacts being a more direct concern than cybersecurity impacts, consider the implementation link to PR.AC-3.** | * **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 software platforms and applications that support offshore operations is critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **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 are critical to ensuring the necessary activities are happening when and as intended. In the personnel safety context, they not only apply to human communications and data flow, but also communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to personnel safety impacts are identified. Consider frequent communications that are contained on the vessel or facility, external communications, such as those necessary to support GPS navigation, and intermittent or continuous communication and data flow between offshore 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-4: External information systems are catalogued | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO02.02 * ISO/IEC 27001:2013 A.11.2.6 * NIST SP 800-53 Rev. 4 AC-20, SA-9 | EDM-1a, -1c, -1e, -1g,  RM-1c |
| 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 personnel safety impacts of offshore operations resources 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, such as rig POC, vendor POC, operator POC, drilling contractor POC and establishing the most critical roles and responsibilities for the organization first.** | * **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-2: Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 * ISO/IEC 27001:2013 A.6.1.4 * NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 | TVM-1a, -1b, -2a, -2b |
| 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 and OT technologies employed in an offshore operating 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. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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** | **To protect personnel safety during offshore operations, risks that impact personnel safety must be identified as such, and those personnel safety 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 personnel safety, “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** |
| Risk Management Strategy | **ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders** | **Addressing personnel safety risks during offshore 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-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies transportation systems, which includes parts of the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[3]](#footnote-3) Protecting personnel is critical to the viability of continued offshore operations. Operations that result in one or more significant harms to individuals will be impeded or even halted, based on the severity of the 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 | Access controls, awareness and training, and maintenance were identified as the priority activities. Without access control, knowledge of personnel’s location is inhibited. Without awareness and training, personnel are not prepared to manage a personnel security incident. Without maintenance, systems will not be ready to deal with personnel safety issues. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-2, PR.AC-5** | PR.AC-3 |
| Awareness and Training | **PR.AT-1, PR.AT-3, PR.AT-5** |  |
| Maintenance |  | PR.MA-1, PR.MA-2 |
| Protective Technology | **PR.PT-2, 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-2: Physical access to assets is managed and protected** | **Physical access to offshore 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 industry-wide impacts, and may lead to issues that span other Mission Objectives, such as Maintaining Environmental Safety and Maintain Reliability. The high prioritization stems from the need for appropriately restricting access to things that can cause danger. For example, restricting access to cables, control cabinets, and heavy machinery. Impact is likely to be greater on drilling and production facilities than in vessels.** | * **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-3: Remote access is managed | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01, DSS01.04, DSS05.03 * ISA 62443-2-1:2009 4.3.3.6.6 * ISA 62443-3-3:2013 SR 1.13, SR 2.6 * ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 | IAM-2a, -2b, -2c, -2d,  -2e, -2f, -2g |
| Access Control | **PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate** | **Network segregation is one of the most impactful and efficient activities for protecting critical systems, such as process control systems and navigation systems (e.g., GPS, dynamic positioning). Segmentation requires adequate planning and budgeting to support the unique needs of each organization’s network design and needs (e.g., nature of vendor access to support operations).** | * **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 offshore 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 offshore operations rely heavily on a diverse contractor base to function. All personnel on offshore facilities and vessels, 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 facility or 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 offshore 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** |
| Maintenance | PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | ***Rationale only provided for High Priority Subcategories*** | * 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-2: Removable media is protected and its use restricted according to policy** | **Use of removeable media on offshore facilities and vessels is one of the most significant issues in offshore operations because it can introduce unknown files and executables into the environment. However, some use of removable media may be critical to certain assets, such as in the case of updating control system software. Organizations should define appropriate parameters for removable media use, including activities such as restricting use to approved media owned and managed by the organization, restricting who can use removable media, and disabling use when practicable.** | * **COBIT 5 DSS05.02, APO13.01** * **ISA 62443-3-3:2013 SR 2.3** * **ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9** * **NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7** | **IAM-2a, -2b, -2c, -3e,  -3f** |
| Protective Technology | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Offshore operations facilities can be large, with a high number of individuals filling many types of roles. Personnel access should be carefully managed to prevent accidents and other unintended consequences to networks, systems, and assets. For example, the chef does not need access to the control room. Physical aspects of this activity should be considered when designing new facilities and vessels.** | * **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 | Real-time awareness of monitoring systems and alerts are critical to personnel safety, with capabilities in this area expanding as organizations mature. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events |  | DE.AE-3, DE.AE-4, DE.AE-5 |
| Security Continuous Monitoring | **DE.CM-8** | DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-7 |
| Detection Processes | **DE.DP-4** | DE.DP-1 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Anomalies and Events | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* | * ISA 62443-3-3:2013 SR 6.1 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4 | IR-1e, -1f, -2i |
| Anomalies and Events | DE.AE-4: Impact of events is determined | *Rationale only provided for High Priority Subcategories* | * 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 | *Rationale only provided for High Priority Subcategories* | * 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, -2j,  TVM-1d,  SA-2d |
| Security Continuous Monitoring | DE.CM-1: The network is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* | * 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, -2b, -2e, -2f,  -2g, -2i,  TVM-1d |
| Security Continuous Monitoring | DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1:2009 4.3.3.3.8 * NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20 | SA-2a, -2b, -2e, -2i |
| 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 |
| Security Continuous Monitoring | DE.CM-4: Malicious code is detected | *Rationale only provided for High Priority Subcategories* | * CCS CSC 5 * COBIT 5 DSS05.01 * ISA 62443-2-1:2009 4.3.4.3.8 * ISA 62443-3-3:2013 SR 3.2 * ISO/IEC 27001:2013 A.12.2.1 * NIST SP 800-53 Rev. 4 SI-3 | SA-2a, -2b, -2e, -2i, CPM-4a |
| Security Continuous Monitoring | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | *Rationale only provided for High Priority Subcategories* | * 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 |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** |
| Detection Processes | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability | *Rationale only provided for High Priority Subcategories* | * CCS CSC 5 * COBIT 5 DSS05.01 * ISA 62443-2-1:2009 4.4.3.1 * ISO/IEC 27001:2013 A.6.1.1 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 | WM-1a, -1d, -1f |
| Detection Processes | **DE.DP-4: Event detection information is communicated to appropriate parties** | **Understanding which events require communication to responsible parties internally and externally and when they should be reported helps ensure the timely evaluation and escalation to Response activities when appropriate. Procedures should include considerations for communicating unintentional discoveries, which may also provide important event information.**  **Note that DE.DP-4 assumes implementation of DE.DP-1.** | * **COBIT 5 APO12.06** * **ISA 62443-2-1:2009 4.3.4.5.9** * **ISA 62443-3-3:2013 SR 6.1** * **ISO/IEC 27001:2013 A.16.1.2** * **NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4** | **IR-1b, -3c, -3n,**  **ISC-1a, -1c, -1d, -1h,  -1j** |

| Respond | Proper response and communication plan development and utilization is critical in the response phase of maintaining personnel 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** |  |
| Communications | **RS.CO-1, RS.CO-4** |  |
| Analysis |  | RS.AN-1 |
| Mitigation | **RS.MI-1, RS.MI-2** |  |

| 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 help 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** |
| Communications | **RS.CO-1: Personnel know their roles and order of operations when a response is needed** | **Effective and efficient response to a cybersecurity event requires that all IT and OT personnel know and understand their role prior to response activities commencing. For cybersecurity events that may impact personnel safety, timing can be critical. Failure to properly execute response procedures quickly, adequately, and in the correct order can result in issues ranging from minor harms to death.** | * **ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** * **ISO/IEC 27001:2013 A.6.1.1, A.16.1.1** * **NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8** | **IR-3a, -5b** |
| Communications | **RS.CO-4: Coordination with stakeholders occurs consistent with response plans** | **Responding to a cybersecurity event takes coordination across multiple parts of the business to ensure the right activities can be conducted at the right time. Response plans describe the minimum activities that must be coordinated between stakeholders for a successful response to a cybersecurity event.** | * **ISA 62443-2-1:2009 4.3.4.5.5** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8** | **IR-3d, -5b** |
| Analysis | RS.AN-1: Notifications from detection systems are investigated | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS02.07 * 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 6.1 * ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4 | IR-1e, -1f |
| Mitigation | **RS.MI-1: Incidents are contained** | **Failure to contain IT and OT cybersecurity-related events may result in safety, operational, or compliance issues that limit or prevent the organization’s ability to protect personnel. Containment activities may be driven in part by legal and regulatory requirements as well as industry standards. Particularly for physical systems, earlier response activities are more likely to focus on containment measures before mitigation measures.** | * **ISA 62443-2-1:2009 4.3.4.5.6** * **ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4** * **ISO/IEC 27001:2013 A.16.1.5** * **NIST SP 800-53 Rev. 4 IR-4** | **IR-3h** |
| Mitigation | **RS.MI-2: Incidents are mitigated** | **Unmitigated IT and OT cybersecurity-related events may result in safety, operational, or compliance issues that limit or prevent the organization’s ability to protect personnel. Incident mitigation activities may be driven in part by legal and regulatory requirements as well as industry standards.** | * **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10** * **ISO/IEC 27001:2013 A.12.2.1, A.16.1.5** * **NIST SP 800-53 Rev. 4 IR-4** | **IR-3b** |

| Recover | When incidents occur that impact personnel safety, Recovery planning and communications are required even though there are no High Priority Subcategories. Recovery planning helps organizations get back to a desirable state of operation. Managing public relations and reputation after incidents helps ensure accurate messaging is communicated externally. If a safety system fails but no personnel issues happen, RC.CO-3 is more important than RC.CO-1 and RC.CO-2. | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Recovery Planning |  | RC.RP-1 |
| Communications |  | RC.CO-1, RC.CO-2 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Recovery Planning | RC.RP-1: Recovery plan is executed during or after an event | *Rationale only provided for High Priority Subcategories* | * CCS CSC 8 * COBIT 5 DSS02.05, DSS03.04 * ISO/IEC 27001:2013 A.16.1.5 * NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 | IR-3b, -3d, -3o, -4k |
| Communications | RC.CO-1: Public relations are managed | *Rationale only provided for High Priority Subcategories* | • COBIT 5 EDM03.02 | RM-1c |
| Communications | RC.CO-2: Reputation after an event is repaired | *Rationale only provided for High Priority Subcategories* | • COBIT 5 MEA03.02 | IR-3d |

## **B-2 Mission Objective 2: Maintain Environmental Safety**

|  |
| --- |
| ***Mission Objective 2: Maintain Environmental Safety***  Recognizing cybersecurity-effects on process control systems that impact environmental safety. Preventing harm to the environments and ecosystems through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. 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 offshore operations * implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management, risk assessment and risk management processes are the primary method used to identify procedures, technologies, and equipment 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 as a result of risk assessments. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID-AM-1, ID.AM-2, ID.AM-3, ID.AM-5, ID.AM-6** | ID.AM-4 |
| Risk Assessment | **ID.RA-5,** **ID.RA-6** | ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4 |
| Risk Management Strategy | **ID.RM-1, ID.RM-3** |  |

| 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 offshore operations is a foundational activity that supports:**   * **identifying and prioritizing assets that have environmental safety impacts** * **recognizing specific equipment that is being effected and effectively responding during an incident** * **understanding gaps in redundancy and failover (Response Subcategories become more important without adequate redundancy and failover)**     **With physical impacts being a more direct concern than cybersecurity impacts, consider the implementation link to PR.AC-3.** | * **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 software platforms and applications that support offshore operations is critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **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 are critical to ensuring the necessary activities are happening when and as intended. In the environmental safety context, they apply to communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to environmental safety impacts are identified. Consider frequent communications that are contained on the vessel or facility, external communications, such as those necessary to support GPS navigation, and intermittent communications, such as when a vessel arrives at port. All critical offshore operations activities that involve intermittent or continuous communication and data flow between offshore and onshore facilities should be protected.** | * **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-4: External information systems are catalogued | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO02.02 * ISO/IEC 27001:2013 A.11.2.6 * NIST SP 800-53 Rev. 4 AC-20, SA-9 | EDM-1a, -1c, -1e, -1g,  RM-1c |
| 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 offshore operations resources 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, such as rig POC, vendor POC, operator POC, drilling contractor POC and establishing the most critical roles and responsibilities for the organization first.** | * **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-2: Threat and vulnerability information is received from information sharing forums and sources | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 * ISO/IEC 27001:2013 A.6.1.4 * NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 | TVM-1a, -1b, -2a, -2b |
| 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 |
| *Rationale only provided for High Priority Subcategories* | 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 an offshore operating 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 environmental safety needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect environmental safety, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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** | **To protect environmental safety during offshore operations, risks that impact environmental safety must be identified as such, and those environmental safety 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.[[4]](#footnote-4) For risks that impact environmental safety, “accept” may only be an appropriate option under limited circumstances.[[5]](#footnote-5) 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** |
| Risk Management Strategy | **ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders** | **Addressing environmental safety risks during offshore 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-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies transportation systems, which includes parts of the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[6]](#footnote-6) Protecting the environment is critical to the viability of continued offshore 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 | Access controls, training, good maintenance programs and proper deployment of protective technology are critical to maintaining environmental safety. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-2, PR.AC-5** |  |
| Awareness and Training | **PR.AT-1, PR.AT-3, PR.AT-5** |  |
| Maintenance |  | PR.MA-1, PR.MA-2 |
| Protective Technology | **PR.PT-2, 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-2: Physical access to assets is managed and protected** | **Physical access to offshore 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 industry-wide impacts, and may lead to issues that span other Mission Objectives, such as Maintaining Environmental Safety and Maintain Reliability. The high prioritization stems from the need for appropriately restricting access to things that can cause danger. For example, restricting access to cables, control cabinets, and heavy machinery. Impact is likely to be greater on drilling and production facilities than in vessels.** | * **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-5: Network integrity is protected, incorporating network segregation where appropriate** | **Network segregation is one of the most impactful and efficient activities for protecting critical systems, such as process control systems and navigation systems (e.g., GPS, dynamic positioning). Segmentation requires adequate planning and budgeting to support the unique needs of each organization’s network design and needs (e.g., nature of vendor access to support operations).** | **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 offshore operations training accountability. Cybersecurity incidents can impact safety, making training critical for preventing environmental 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 offshore operations rely heavily on a diverse contractor base to function. All personnel on offshore facilities and vessels, 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 facility or 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 offshore 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** |
| Maintenance | PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | *Rationale only provided for High Priority Subcategories* | * 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-2: Removable media is protected and its use restricted according to policy** | **Use of removeable media on offshore facilities and vessels is one of the most significant issues in offshore operations because it can introduce unknown files and executables into the environment. However, some use of removable media may be critical to certain assets, such as in the case of updating control system software. Organizations should define appropriate parameters for removable media use, including activities such as restricting use to approved media owned and managed by the organization and disabling use when practicable.** | * COBIT 5 DSS05.02, APO13.01 * ISA 62443-3-3:2013 SR 2.3 * ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 * NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 | **IAM-2a, -2b, -2c, -3e,  -3f** |
| Protective Technology | **PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality** | **Offshore operations facilities can be large, with a high number of individuals filling many types of roles. Personnel access should be carefully managed to prevent accidents and other unintended consequences to networks, systems, and assets. For example, the chef does not need access to the control room. Physical aspects of this activity should be considered when designing new facilities and vessels.** | * **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 | Real time awareness of monitoring systems and alerts are critical to environmental safety, with capabilities in this area expanding as organizations mature. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events |  | DE.AE-3, DE.AE-4, DE.AE-5 |
| Security Continuous Monitoring | **DE.CM-8** | DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-7 |
| Detection Processes | DE.DP-4 | DE.DP-1 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Anomalies and Events | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-3-3:2013 SR 6.1 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4 | IR-1e, -1f, -2i |
| Anomalies and Events | DE.AE-4: Impact of events is determined | ***Rationale only provided for High Priority Subcategories*** | * 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 | ***Rationale only provided for High Priority Subcategories*** | * 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, -2j,  TVM-1d,  SA-2d |
| Security Continuous Monitoring | DE.CM-1: The network is monitored to detect potential cybersecurity events | ***Rationale only provided for High Priority Subcategories*** | * 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, -2b, -2e, -2f,  -2g, -2i,  TVM-1d |
| Security Continuous Monitoring | DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-2-1:2009 4.3.3.3.8 * NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20 | SA-2a, -2b, -2e, -2i |
| 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 |
| Security Continuous Monitoring | DE.CM-4: Malicious code is detected | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 5 * COBIT 5 DSS05.01 * ISA 62443-2-1:2009 4.3.4.3.8 * ISA 62443-3-3:2013 SR 3.2 * ISO/IEC 27001:2013 A.12.2.1 * NIST SP 800-53 Rev. 4 SI-3 | SA-2a, -2b, -2e, -2i, CPM-4a |
| Security Continuous Monitoring | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | ***Rationale only provided for High Priority Subcategories*** | * 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 |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** |
| Detection Processes | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 5 * COBIT 5 DSS05.01 * ISA 62443-2-1:2009 4.4.3.1 * ISO/IEC 27001:2013 A.6.1.1 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 | WM-1a, -1d, -1f |
| Detection Processes | **DE.DP-4: Event detection information is communicated to appropriate parties** | **Understanding which events require communication to responsible parties internally and externally and when they should be reported helps ensure the timely evaluation and escalation to Response activities when appropriate. Procedures should include considerations for communicating unintentional discoveries, which may also provide important event information.**  **Note that DE.DP-4 assumes implementation of DE.DP-1.** | * **COBIT 5 APO12.06** * **ISA 62443-2-1:2009 4.3.4.5.9** * **ISA 62443-3-3:2013 SR 6.1** * **ISO/IEC 27001:2013 A.16.1.2** * **NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4** | **IR-1b, -3c, -3n,**  **ISC-1a, -1c, -1d, -1h,  -1j** |

| Respond | Proper response and communication plan development and utilization is critical in the response phase of maintaining personnel 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** |  |
| Communications | **RS.CO-1, RS.CO-4** |  |
| Analysis |  | RS.AN-1 |
| Mitigation | **RS.MI-1, RS.MI-2** |  |

| 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 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** |
| Communications | **RS.CO-1: Personnel know their roles and order of operations when a response is needed** | **Effective and efficient response to a cybersecurity event requires that all IT and OT personnel know and understand their role prior to response activities commencing. For cybersecurity events that may impact environmental safety, timing can be critical. Failure to properly execute response procedures quickly, adequately, and in the correct order can result in issues ranging from minor harms to death.** | * **ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** * **ISO/IEC 27001:2013 A.6.1.1, A.16.1.1** * **NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8** | **IR-3a, -5b** |
| Communications | **RS.CO-4: Coordination with stakeholders occurs consistent with response plans** | **Responding to a cybersecurity event takes coordination across multiple parts of the business to ensure the right activities can be conducted at the right time. Response plans describe the minimum activities that must be coordinated between stakeholders for a successful response to a cybersecurity event.** | * **ISA 62443-2-1:2009 4.3.4.5.5** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8** | **IR-3d, -5b** |
| Analysis | RS.AN-1: Notifications from detection systems are investigated | ***Rationale only provided for High Priority Subcategories*** | * COBIT 5 DSS02.07 * 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 6.1 * ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4 | IR-1e, -1f |
| Mitigation | **RS.MI-1: Incidents are contained** | **Failure to contain IT and OT cybersecurity-related events may result in safety, operational, or compliance issues that limit or prevent the organization’s ability to protect the environment. Containment activities may be driven in part by legal and regulatory requirements as well as industry standards. Particularly for physical systems, earlier response activities are more likely to focus on containment measures before mitigation measures.** | * **ISA 62443-2-1:2009 4.3.4.5.6** * **ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4** * **ISO/IEC 27001:2013 A.16.1.5** * **NIST SP 800-53 Rev. 4 IR-4** | **IR-3h** |
| Mitigation | **RS.MI-2: Incidents are mitigated** | **Unmitigated IT and OT cybersecurity-related events may result in safety, operational, or compliance issues that limit or prevent the organization’s ability to protect the environment. Incident mitigation activities may be driven in part by legal and regulatory requirements as well as industry standards.** | * **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10** * **ISO/IEC 27001:2013 A.12.2.1, A.16.1.5** * **NIST SP 800-53 Rev. 4 IR-4** | **IR-3b** |

| Recover | When incidents occur that impact personnel safety, recovery planning and communications are required even though there are no High Priority Subcategories. Recovery planning helps organizations get back to a desirable state of operation. Managing public relations and reputation after incidents helps ensure accurate messaging is communicated externally. If a safety system fails but no personnel issues happen, RC.CO-3 is more important that RC.CO-1 and RC.CO-2. | |
| --- | --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Recovery Planning |  | RC.RP-1 |
| Communications |  | RC.CO-1, RC.CO-2 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Recovery Planning | RC.RP-1: Recovery plan is executed during or after an event | ***Rationale only provided for High Priority Subcategories*** | * CCS CSC 8 * COBIT 5 DSS02.05, DSS03.04 * ISO/IEC 27001:2013 A.16.1.5 * NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 | IR-3b, -3d, -3o, -4k |
| Communications | RC.CO-1: Public relations are managed | ***Rationale only provided for High Priority Subcategories*** | • COBIT 5 EDM03.02 | RM-1c |
| Communications | RC.CO-2: Reputation after an event is repaired | ***Rationale only provided for High Priority Subcategories*** | • COBIT 5 MEA03.02 | IR-3d |

## **B-3 Mission Objective 3: Maintain Reliability**

|  |
| --- |
| ***Mission Objective 3: Maintain Reliability***  Preserving systems integrity so that they function as designed and intended throughout their planned life. Prevention of accidents and adverse business impacts through: Risk Assessment; Anomaly Detection; Asset Management; and Protective Technology. Organizations should:   * manage risks to reliability using a structured process * examine components that can cause failure alone or in combination * design IT and OT integration points to fail safely within the system’s operational environment * preserve a steady state of containment when not in operation |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management and risk assessment processes are the primary method used to identify procedures, technologies, and equipment that support the organization’s ability to maintain reliability. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID-AM-1, ID.AM-2, ID.AM-5, ID.AM-6** | ID.AM-4 |
| Risk Assessment | **ID.RA-3, ID.RA-5,** **ID.RA-6** | ID.RA-1, 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** | **Maintaining a current inventory of the physical devices and systems that support offshore operations provides the foundation for identifying and prioritizing assets that are most critical to maintaining the reliability of offshore 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 software platforms and applications that support offshore operations is critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **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-4: External information systems are catalogued | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO02.02 * ISO/IEC 27001:2013 A.11.2.6 * NIST SP 800-53 Rev. 4 AC-20, SA-9 | EDM-1a, -1c, -1e, -1g  RM-1c |
| 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 reliability impacts to offshore operations resources are necessary factors to consider when prioritizing resources. For example, taking a monitoring system offline may lead to a failure to identify issues that can impact reliability. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. 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, such as rig POC, vendor POC, operator POC, drilling contractor POC, and establishing the most critical roles and responsibilities for the organization first.** | * **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 to plan for addressing potential incidents related to those specific threats if the risks associated with them are realized.** | * **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 an offshore operating 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 reliability needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect reliability, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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 | Access controls, training, good maintenance programs and proper deployment of protective technology are critical to maintaining reliability. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-2** | PR.AC-1, PR.AC-3, PR.AC-4 |
| Information Protection Processes & Procedures | **PR.IP-1, PR.IP-2,** **PR.IP-3, PR.IP-9**, **PR.IP-12** | PR.IP-10 |
| Maintenance | **PR.MA-1, PR.MA-2** |  |
| 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** | **Physical access to offshore 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 industry-wide impacts, and may lead to issues that span other Mission Objectives, such as Maintaining Personnel Safety and Maintaining Environmental Safety. While physical access is the primary threat to offshore assets in many instances, physical access controls must be supplemented with logical access controls when non-physical access is required.** | * **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-3: Remote access is managed | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01, DSS01.04, DSS05.03 * ISA 62443-2-1:2009 4.3.3.6.6 * ISA 62443-3-3:2013 SR 1.13, SR 2.6 * ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 | 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 | *Rationale only provided for High Priority Subcategories* | * 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-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-2: A System Development Life Cycle to manage systems is implemented** | **System Development Life Cycles promote a structured set of processes and approaches to identifying and documenting the needs and purpose of the system, system requirements and architecture, design and development considerations, decisions regarding system integration, testing/evaluating success of requirements implementation, and managing the on-going operations and maintenance of the system, and system retirement. Following consistent methodologies supports reliability by limiting the potential for deviating from vetted organizational requirements and standards to limit adverse impacts to the offshore operating environment.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.3** * **ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5** * **NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8** | **ACM-3d** |
| 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 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 to the offshore operating environment.** | * **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 & Procedures | **PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed** | **Offshore 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 they are periodically updated, allowing the organization to maintain an acceptable level of preparedness. This activity supports response and recovery activities so that offshore operations can return to a reliable state expediently. PR.IP-9 assumes PR.IP-10 is addressed. 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** |
| Information Protection Processes & Procedures | PR.IP-10: Response and recovery plans are tested | *Rationale only provided for High Priority Subcategories* | * 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-12: A vulnerability management plan is developed and implemented** | **Understanding and managing vulnerabilities are a key part of risk assessments and management. Implementing vulnerability management plans includes scanning tools and techniques for vulnerabilities (when scanning will not impact reliability of systems, particularly OT systems) and remediating vulnerabilities in accordance with organizational risk assessments. Organizational and system risk posture guide the frequency and thoroughness of vulnerability scans. Vulnerability management plans include processes for authorizing personnel as needed, to conduct scans and implement required fixes. PR.IP-12 and PR.IP-9 should be developed and maintained with coordination.** | * **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** |
| 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 offshore assets safeguards against preventable issues that could impact operational reliability. 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.** | * **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** | **Offshore operations assets are by their nature not readily accessible by those not physically present on an offshore facility or vessel. Remote maintenance requires a network connection to access the supported system or device, which can offer convenience and flexibility yet also expose assets to new vulnerabilities that physical security protections cannot address. Restricting access for remote maintenance to only approved support professionals and activities, and logging activities minimizes the risk of incidents occurring when the availability to perform remote maintenance is necessary.**  **Also consider restricting access for the maintenance communication channels.** | * **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,  -2f, -2g, -2h** |
| Protective Technology | **PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy** | **Audit/log records provide a history of activities and maintenance performed on a system or device. These records can provide input into monitoring tools, which helps identify security incidents after they have occurred. They can also provide a history of what has transpired during a security incident, which aids in response and recovery efforts that support offshore operations in returning to a reliable state.** | * **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, -2a, 1b, -1c,**  **-2e, -4a, -1d, -1e, -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 limits access to resources to only those that have a need to access a system or asset 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 that 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 offshore operations 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 | Robust detection processes that continuously monitor sensors and alarms for anomalies and events are critical to maintaining operational reliability. If a cyber cause results in a physical effect, a cyber-attack could influence reliability, placing greater emphasis on DE.AE-1, 2, and 3. If a physical cause results in a physical effect, greater emphasis is placed on DE.AE-1, 4, and 5. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5** |  |
| Security Continuous Monitoring | **DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.CM-8** |  |

| 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 typical offshore operations supports operational security by providing a means of comparing current activities against expectations in order 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-2: Detected events are analyzed to understand attack targets and methods** | **Determining whether and how offshore operational components are attacked provides insight into operational impacts that may affect the organization’s ability to maintain reliability.** | * **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-3: Event data are aggregated and correlated from multiple sources and sensors** | **Aggregating and correlating information provides broader situational awareness across assets, systems, offshore facilities and vessels, and the organization than reviewing events from individual audit/log records.** | * **ISA 62443-3-3:2013 SR 6.1** * **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4** | | **IR-1e, -1f, -2i** | |
| Anomalies and Events | **DE.AE-4: Impact of events is determined** | **Knowing the impact of events helps organizations understand the impact to maintaining the reliability of offshore 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 reliability 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 the reliability of offshore operations.** | * **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-2: The physical environment is monitored to detect potential cybersecurity events** | **Monitoring facilities and physical equipment, devices, systems, and other assets for access issues and other activities is one of the primary ways to identify anomalies that can lead to cybersecurity events that impact reliability.** | * **ISA 62443-2-1:2009 4.3.3.3.8** * **NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20** | | **SA-2a, -2b, -2e, -2i** | |
| Security Continuous Monitoring | **DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events** | **Human error and insider threat can cause significant impacts to reliability in offshore operations. Monitoring personnel activity for access issues and other activities is one of the primary ways to identify anomalies that can lead to cybersecurity events that impact reliability.** | * **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** | |
| 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 identify anomalies that can lead to cybersecurity events that impact reliability.** | * **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 offshore operations provide input into event correlation and analysis tools, alert mechanisms, and the response process.** | * **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** | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |

|  |  |  |
| --- | --- | --- |
| 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 |

## **B-4 Mission Objective 4: Maintain Continuity and Integrity of Operations**

|  |
| --- |
| ***Mission Objective 4: Maintain Continuity and Integrity of Operations***  Preserving the ability to operate at the intended level within the desired time frame. System functions without interruption through: Asset Management, Risk Assessment, Access Control, Information Protection Processes and Procedures, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring. Organizations should:   * incorporate outcomes of risk assessments into facility and organizational management systems as well as the systems engineering lifecycle and change management procedures * perform preventative maintenance * plan for backups and work arounds * implement redundancy for critical processes and assets * employ management of change procedures |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management, 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 continuity and integrity of offshore operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID-AM-1, ID.AM-2, ID.AM-5, ID.AM-6** | ID.AM-4 |
| Risk Assessment | **ID.RA-4, ID.RA-6** | ID.RA-1, ID.RA-3, ID.RA-5 |
| 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 offshore 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 software platforms and applications that support offshore operations is critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **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-4: External information systems are catalogued | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO02.02 * ISO/IEC 27001:2013 A.11.2.6 * NIST SP 800-53 Rev. 4 AC-20, SA-9 | EDM-1a, -1c, -1e, -1g,  RM-1c |
| 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 continuity and integrity impacts to offshore operations resources are necessary factors to consider when prioritizing resources. For example, taking a monitoring system offline may lead to a failure to identify issues that can result in a system interruption. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. 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, such as rig POC, vendor POC, operator POC, drilling contractor POC, and establishing the most critical roles and responsibilities for the organization first.** | * **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 | ***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** | **Internal and external business impacts are factors to consider during risk assessments.**  **Internally, understanding business impacts influences specific controls selected to support objectives and how they are implemented. Business impacts consider impacts to and from other third parties, including business partners, service providers, and other contractors, as well as supply chain impacts. This allows traceability from critical business and mission systems to system hardware, software, and firmware components.**  **Externally, business impacts may lead to broader critical infrastructure impacts. For example, severe business impacts to large organizations or supply chains could impact the availability of supplies and services and possibly the Nation’s economy.** | * **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 | ***Rationale only provided for High Priority Subcategories*** | * 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 offshore 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.[[7]](#footnote-7) For risks that impact continuity and integrity of offshore operations, “accept” may only be an appropriate option under limited circumstances.[[8]](#footnote-8) 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** |
| 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 offshore 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** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies transportation systems, which includes parts of the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[9]](#footnote-9)**  **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 planning, processes, maintenance and protective technologies are key to maintaining continuity and integrity of operations.* | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Information Protection Processes & Procedures | **PR.IP-1, PR.IP-3,** **PR.IP-4, PR.IP-9** | PR.IP-2, PR.IP-5, PR.IP-10 |
| 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 |
| Information Protection Processes and 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 enable continuity and integrity. Baselines also support response and recovery efforts in returning to a desired operating state after an incident.** | * **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-2: A System Development Life Cycle to manage systems is implemented | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01 * ISA 62443-2-1:2009 4.3.4.3.3 * ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 * NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8 | ACM-3d |
| 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 each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports continuity and integrity of operations 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 so as limit adverse impacts to the offshore operating environment.** | * **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 quality backups are available when needed. Testing should be periodically conducted to ensure 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-5: Policy and regulations regarding the physical operating environment for organizational assets are met | *Rationale only provided for High Priority Subcategories* | * 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 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** | **Offshore 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 they are periodically updated, allowing the organization to maintain an acceptable level of preparedness. This activity supports response and recovery activities so that offshore 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** |
| Information Protection Processes and Procedures | PR.IP-10: Response and recovery plans are tested | *Rationale only provided for High Priority Subcategories* | * 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, -3k, -4f, -4i, -4j |
| 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 offshore assets safeguards against preventable issues that could impact the continuity and integrity of operations. 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.** | * **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 | *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 | *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 | Detection activities help identify issues that may impeded the organization’s ability to maintain the continuity and integrity of operations | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-1, DE.AE-4** | DE.AE-3 |
| Security Continuous Monitoring | **DE.CM-8** | DE.CM-1, DE.CM-2, DE.CM-3 |
| Detection Processes | **DE.DP-1** | DE.DP-2, DE.DP-4, DE.DP-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 typical offshore operations supports operational security by providing a means of comparing current activities against expectations in order to identify anomalies or other events that may require analysis and response. DE.AE‑1 assumed implementation of DE.AE‑5.** | * **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-3: Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* | * ISA 62443-3-3:2013 SR 6.1 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4 | IR-1e, -1f, -2i |
| 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 offshore 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** |
| Security Continuous Monitoring | DE.CM-1: The network is monitored to detect potential cybersecurity events | ***Rationale only provided for High Priority Subcategories*** | * 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, -2b, -2e, -2f,  -2g, -2i,  TVM-1d |
| Security Continuous Monitoring | DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-2-1:2009 4.3.3.3.8 * NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20 | SA-2a, -2b, -2e, -2i |
| 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 |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** |
| Detection Processes | **DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability** | **Detection activities identify incidents that may impact the integrity and continuity of offshore operations. Ensuring accountable individuals are assigned roles and responsibilities for detection activities increases the likelihood of performing these activities effectively. For example, assigning responsibility to look for signs of an incident when performing routine maintenance improves the likelihood of detecting an incident. Collaboration between points-of contact (POCs) is important. At a minimum, consider defining roles and responsibilities for critical POCs, such as rig POC, vendor POC, operator POC, drilling contractor POC, and establishing the most critical roles and responsibilities for the organization first.** | * **CCS CSC 5** * **COBIT 5 DSS05.01** * **ISA 62443-2-1:2009 4.4.3.1** * **ISO/IEC 27001:2013 A.6.1.1** * **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14** | **WM-1a, -1d, -1f** |
| Detection Processes | DE.DP-2: Detection activities comply with all applicable requirements | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1:2009 4.4.3.2 * ISO/IEC 27001:2013 A.18.1.4 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 | IR-1d, 5a, -1g, -5f,  TVM-1d,  RM-1c,  RM-2j |
| Detection Processes | DE.DP-4: Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.06 * ISA 62443-2-1:2009 4.3.4.5.9 * ISA 62443-3-3:2013 SR 6.1 * ISO/IEC 27001:2013 A.16.1.2 * NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 | IR-1b, -3c, -3n,  ISC-1a, -1c, -1d, -1h,  -1j |
| Detection Processes | DE.DP-5: Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO11.06, DSS04.05 * ISA 62443-2-1:2009 4.4.3.4 * ISO/IEC 27001:2013 A.16.1.6 * NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 | IR-3h, -3k |

|  |  |  |
| --- | --- | --- |
| Respond | Response planning positions organizations to effectively address incidents that impact the continuity and integrity of operations. | |
| 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 help protect the organization’s resources, including those that may impact the continuity and integrity of operations.** | * **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 | Recovery planning and adapting capabilities based on field experience are key to maintaining continuity and integrity of operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Recovery Planning | **RC.RP-1** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Recovery Planning | **RC.RP-1: Recovery plan is executed during or after an event** | **Recovery plans help organizations move past the initial response phase post-incident and focus instead on coordinated activities to restore capabilities to the desired operating level. Recovery plans include prioritization of activities and assets based on mission and business criticality. Organizations coordinate withthird parties, including business partners, service providers, and other contractors, as well as supply chain partners as needed.** | * **CCS CSC 8** * **COBIT 5 DSS02.05, DSS03.04** * **ISO/IEC 27001:2013 A.16.1.5** * **NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8** | **IR-3b, -3d, -3o, -4k** |

## **B-5 Mission Objective 5: Maintain Cyber Situational Awareness**

|  |
| --- |
| ***Mission Objective 5: Maintain Cyber Situational Awareness***  Understanding and assessing cyber threats and vulnerabilities and the operational risks to which they can lead. System parameters are maintained within operational norms through: Risk Assessment, Awareness and Training, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes. Organizations should:   * employ appropriate administrative, technical, and physical controls to protect IT and OT capabilities from potential adverse cyber-effects * monitor changes to technologies in use (e.g., vendor updates to software) * engage with communities that promote awareness of industry-specific threats and vulnerabilities (e.g., InfraGard, information sharing and analysis organizations that support the organization’s industry and or geographical locations) * provide adequate cybersecurity training to personnel, based on their role(s) |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management and risk assessment processes are the primary method used to identify procedures, technologies, and equipment that support the organization’s ability to maintain cyber situational awareness. | |
| Categories | **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 to 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 an offshore operating 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 cyber situational awareness needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect reliability, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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.**  **ID.RA-5 assumes implementation of ID.RA-4.** | * **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** | **As risks are identified, their 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.[[10]](#footnote-10) 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 offshore operations requires awareness and training activities, supporting processes and procedures, and protective technologies. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1, PR.AT-3** | PR-AT-5 |
| Information Protection Processes and Procedures | **PR.IP-1, PR.IP-2, PR.IP-5, PR.IP-7, PR.IP-11** |  |
| Protective Technology | **PR.PT-1, 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 roles, responsibilities, and requirements necessary to support offshore operations training accountability. Cybersecurity incidents can impact safety, making training critical for supporting the ability to maintain adequate cyber situational awareness.** | * **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 offshore operations rely heavily on a diverse contractor base to function. All personnel on offshore facilities and vessels, regardless of which organization employs them directly, must understand their roles and responsibilities for maintaining cyber situational awareness the context of the specific operations on their facility or 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** | *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** |
| 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 desired operating state. Baselines are also useful for supporting training and awareness efforts by communicating what is normal for the operational environment. Baselines also support response and recovery efforts in returning to a desired operating state after an incident.** | * **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-2: A System Development Life Cycle to manage systems is implemented** | **System Development Life Cycles promote a structured set of processes and approaches to identifying and documenting the needs and purpose of the system, system requirements and architecture, design and development considerations, decisions regarding system integration, testing/evaluating success of requirements implementation, and managing the on-going operations and maintenance of the system, and system retirement. Following consistent methodologies supports the ability to maintain cyber situational awareness by limiting the potential for deviating from vetted organizational requirements and standards so that issues that may cause adverse impacts to the offshore operating environment are more readily recognizable.** | * **COBIT 5 APO13.01** * **ISA 62443-2-1:2009 4.3.4.3.3** * **ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5** * **NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8** | **ACM-3d** |
| 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-7: Protection processes are continuously improved** | **Regularly examining the effectiveness and efficiency of protection processes provides organizations with valuable feedback regarding how their cybersecurity efforts to protect offshore operations assets are performing, and where improvements need to be made over time as problems or improved practices are identified. Additionally, the threat environment for offshore operations may continue to evolve even when organizations do not make signification changes to their environment (e.g., new vulnerabilities for an existing technology may be discovered).** | * **COBIT 5 APO11.06, DSS04.05** * **ISA 62443-2-1:2009 4.4.3.1, 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 SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6** | **CPM-1g** |
| Information Protection Processes & Procedures | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Offshore operations rely on personnel to operate and maintain HR assets, and personnel that fulfill HR requirements commonly have privileged access to sensitive workforce information, such as salary information and performance reviews. 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 integrity 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 HR‑related roles and responsibilities. Including cybersecurity in HR practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with HR-related policies and procedures. Maintaining awareness of personnel changes enables the organization to ensure training and other role-specific cybersecurity needs are met.** | * **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 provide a history of activities and maintenance performed on a system or device. These records can provide input into monitoring tools, which helps identify security incidents after they have occurred. They can also provide a history of what has transpired during a security incident, which aids in response and recovery efforts that support offshore operations in future cyber situational awareness activities.** | * **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-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to offshore operations 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 | Detection processes and continuous monitoring activities to identify anomalies and events are critical aspects of cyber situational awareness. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-1, DE.AE-4, DE.AE-5** | DE.AE-2, DE.AE-3 |
| Security Continuous Monitoring | **DE.CM-6, DE.CM-7, DE.CM-8** |  |
| Detection Processes | **DE.DP-1, DE.DP-5** | DE.DP-2, DE.DP-3 |

| 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 typical offshore operations supports operational security by providing a means of comparing current activities against expectations in order 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-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, -2i, -3h |
| Anomalies and Events | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* | * ISA 62443-3-3:2013 SR 6.1 * NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4 | IR-1e, -1f, -2i |
| Anomalies and Events | **DE.AE-4: Impact of events is determined** | **Knowing the impact of events helps organizations prioritize cyber situational awareness activities as well as understand 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-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 offshore 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** |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** |
| Detection Processes | **DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability** | **Detection activities identify incidents that may impact the integrity and continuity of offshore operations. Ensuring accountable individuals are assigned roles and responsibilities for detection activities increases the likelihood of performing these activities effectively. For example, assigning responsibility to look for signs of an incident when performing routine maintenance improves the likelihood of detecting an incident. Collaboration between points-of contact (POCs) is important. At a minimum, consider defining roles and responsibilities for critical POCs, such as rig POC, vendor POC, operator POC, drilling contractor POC and establishing the most critical roles and responsibilities for the organization first.** | * **CCS CSC 5** * **COBIT 5 DSS05.01** * **ISA 62443-2-1:2009 4.4.3.1** * **ISO/IEC 27001:2013 A.6.1.1** * **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14** | **WM-1a, -1d, -1f** |
| Detection Processes | DE.DP-2: Detection activities comply with all applicable requirements | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1:2009 4.4.3.2 * ISO/IEC 27001:2013 A.18.1.4 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 | IR-1d, 5a, -1g, -5f,  TVM-1d,  RM-1c,  RM-2j |
| Detection Processes | DE.DP-3: Detection processes are tested | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.02 * ISA 62443-2-1:2009 4.4.3.2 * ISA 62443-3-3:2013 SR 3.3 * ISO/IEC 27001:2013 A.14.2.8 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 | IR-3e, -3j |
| Detection Processes | **DE.DP-5: Detection processes are continuously improved** | **Effective cyber situational awareness practices must evolve along with changes to the offshore operating environment. Continuous improvement of detection processes may include activities such as periodic review and update of the continuous monitoring strategy, vulnerability scanning plans, metrics and measures evaluated, and security events correlated.** | * **COBIT 5 APO11.06, DSS04.05** * **ISA 62443-2-1:2009 4.4.3.4** * **ISO/IEC 27001:2013 A.16.1.6** * **NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14** | **IR-3h, -3k** |

|  |  |  |
| --- | --- | --- |
| 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 |

## **B-6 Mission Objective 6: Maintain Personnel Competencies**

|  |
| --- |
| ***Mission Objective 6: Maintain Personnel Competencies***  Ensuring employees have adequate knowledge, skills, and abilities to support operations. Preventing personnel-based cyber incidents which may cause adverse cyber or physical effects through: Asset Management, Business Environment, Governance, Awareness and Training, Information Protection Processes and Procedures, Communications. Organizations should:   * understand how personnel encounters with assets can result in cyber-causes with cyber or physical effects * identify and train personnel on interdependence of cybersecurity with operational responsibilities * employ contract resources for specializations that are not available within the organization * implement operational procedures that limit the possibility of human error where possible |

|  |  |  |
| --- | --- | --- |
| Identify | Personnel competencies needed are shaped by the assets held by the organization, the business environment, and governance requirements. Managing the workforce requires an understanding of internal and external security obligations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-5, ID.AM-6** |  |
| Business Environment | **ID.BE-3** |  |
| Governance | **ID.GV-2** | ID.GV-3 |

| 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. To adequately protect resources, personnel must understand the relative importance of resources and factor that knowledge into their decision-making. 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 personnel to effectively carry 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, such as tig POC, vendor POC, operator POC, drilling contractor POC, and establishing the most critical roles and responsibilities for the organization first.** | * **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** |
| Business Environment | **ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated** | **Effectively protecting offshore operations assets depends on personnel being adequately trained to properly manage and protect 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-3b, -1c** |
| Governance | **ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners** | **Operating certain IT and OT equipment necessitates an adequate degree of knowledge and experience, which can be demonstrated through the achievement of licenses, certifications, and other professional designations. In some cases, a current license is a condition for operating OT equipment. These requirements must be considered when defining and assigning security roles and responsibilities. Similarly, licensing requirements should be considered when making implementation decisions regarding the access controls Subcategories (PR.AC).** | * **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 | *Rationale only provided for High Priority Subcategories* | * COBIT 5 MEA03.01, MEA03.04 * ISA 62443-2-1:2009 4.4.3.7 | AACM-4f,  CPM-2k,  EDM-3f,  IAM-3f,  IR-3n, -5f  ISC-2f,  RM-3f,  SA-4f,  TVM-3f,  WM-5f |

|  |  |  |
| --- | --- | --- |
| Protect | Personnel are often the first or second line of defense for the organization’s resources. Aligning cybersecurity requirements to personnel activities aids the organization in achieving compliance with internal policies and procedures, including completion of training requirements and protection of resources. | |
| 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-11** | PR.IP-9 |

| 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 roles, responsibilities, and requirements necessary to support offshore operations training accountability.** | * **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 offshore operations rely heavily on a diverse contractor base to function. All personnel on offshore facilities and vessels, 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 facility or 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 offshore operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in cybersecurity 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.**  **The selection of PR.AT-5 assumes of PR.AT-2 is being addressed.** | * **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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and  managed | *Rationale only provided for High Priority Subcategories* | * 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,  -5d, -5e, -5f, -5g, -5h,  -5i,  TVM-1d,  RM-1c |
| Information Protection Processes & Procedures | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **Offshore operations rely on personnel to operate and maintain HR assets, and personnel that fulfill HR requirements commonly have privileged access to sensitive workforce information, such as salary information and performance reviews. 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 integrity 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 HR‑related roles and responsibilities. Including cybersecurity in HR practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with HR-related policies and procedures. Maintaining awareness of personnel changes enables the organization to ensure training and other role-specific cybersecurity needs are met.** | * **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 | Controls support personnel in meeting their responsibilities. Where possible, continuous monitoring of controls that enable personnel should be implemented to ensure they maintain their ability to effectively support operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | DE.CM-8 | N/A |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |

|  |  |  |
| --- | --- | --- |
| Respond | Responding in cybersecurity incidents requires careful communication among personnel. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | **RS.CO-1** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Communications | **RS.CO-1: Personnel know their roles and order of operations when a response is needed** | **Effective and efficient response to a cybersecurity event requires that all IT and OT personnel know and understand their role prior to response activities commencing. For cybersecurity events that may impact personnel competencies, timing can be critical. Failure to properly execute response procedures quickly, adequately, and in the correct order can result in issues ranging from minor harms to death.** | * **ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** * **ISO/IEC 27001:2013 A.6.1.1, A.16.1.1** * **NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8** | **IR-3a, -5b** |

|  |  |  |
| --- | --- | --- |
| 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 |

## **B-7 Mission Objective 7: Maintain Consistent and Effective Stakeholder Communications**

|  |
| --- |
| ***Mission Objective 7: Maintain Consistent and Effective Stakeholder Communications***  Ensuring critical stakeholders are aware of operational environment. Supporting reliable and valuable communication with the right stakeholders at the right time through: Business Environment, Governance, Risk Management Strategy, Access Control, Information Protection Processes and Procedures, Communications. Organizations should:   * identify stakeholders and establish all critical communication paths * manage reputation through clear, consistent messaging * implement communications procedures for supply chain partners and external entities related to response and recovery efforts when issues arise |

|  |  |  |
| --- | --- | --- |
| Identify | The business environment as well as governance and risk management practices shape the stakeholder communications needs of offshore operations organization. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-2, ID.BE-3** | ID.BE-4 |
| Governance | **ID.GV-2, ID.GV-3** |  |
| Risk Management | **ID.RM-1** | ID.RM-2, ID.RM-3 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Business Environment | **ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies energy systems, which includes the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[11]](#footnote-11) Each organization should understand its role as part of the critical infrastructure and ensure stakeholders understand their individual and collective roles in supporting critical infrastructure activities.** | * **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** | **Effectively protecting offshore 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 | *Rationale only provided for High Priority Subcategories* | * 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,  RM-1c |
| Governance | **ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners** | **Effective communications rely on getting the right information to the right stakeholders at the right time, and the ability of those stakeholders to consume the information and react appropriately. Operating certain IT and OT equipment necessitates an adequate degree of knowledge and experience, which can be demonstrated through the achievement of licenses, certifications, and other professional designations. In some cases, a current license is a condition for operating OT equipment. These requirements must be considered when defining and assigning security roles and responsibilities, and may also help when determining how to align stakeholders with communications. Similarly, licensing requirements should be considered when making implementation decisions regarding the access controls Subcategories (PR.AC).** | * **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 offshore operations activities may be driven or influenced by multiple laws, Executive Orders, 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.**  **Additionally, protecting workforce information from loss, theft, or other compromises ensures the organization can meet these requirements. Protecting workforce information also prevents harms to individuals, such as identity theft or embarrassment, and harms to the organization, such as diversion of resources away from operational objectives or employee distractions due to dealing with identify theft.**  **Policies and practices of organizations may vary. When working with third parties, a formal agreement that clearly describes expectations for information governance between all the parties should be executed.** | * **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** |
| Risk Management Strategy | **ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders** | **Consistent and effective stakeholder communications for offshore operations 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 | ***Rationale only provided for High Priority Subcategories*** | * NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 | RM-1b, -1c |

|  |  |  |
| --- | --- | --- |
| Protect | The ability to demonstrate adequate protection of resources and equipment during an inspection or audit relies heavily on well documented policies and procedures and adequate awareness and training activities. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-1** |  |
| Information Protection Processes & Procedures | **PR.IP-5, PR.IP-9, PR.IP-12** |  |

| 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 assuring 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.**  **The selection of PR.AC-1 assumes PR.AC-2 and PR.AC-3 are being addressed.** | * **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** |
| Information Protection Processes & Procedures | **PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** | **Consistent and effective internal and external stakeholder communications address communication of offshore operations policies, including those that govern the implementation of regulations.** | * **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** | **Offshore 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 communications processes enables organizations to more effectively respond and coordinate with third parties as needed as well as carefully manage external messaging when needed.** | * **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-12: A vulnerability management plan is developed and implemented** | **Vulnerability management plans include linkages to stakeholder communications plans. In offshore operations, vulnerabilities may be identified that are internal to the organization or external to the organization. Communications with external parties, such as services providers, contractors, and other outsourced entities are critical to determining how to effectively address those vulnerabilities. Additionally, offshore facilities and vessels may have a need to communicate with onshore entities for coordination regarding identified vulnerabilities and plans for addressing them. Communications regarding vulnerability management plans may address known vulnerabilities for a specific system or asset, or may be provided for informational purposes to address similar vulnerabilities on other assets.** | * **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 | Communications permeate many aspects of cybersecurity. Where possible, continuous monitoring of controls that enable communications should be implemented to ensure communications can occur uninterrupted. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-8** | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** |

|  |  |  |
| --- | --- | --- |
| Respond | When organizations experience a cybersecurity events, stakeholder communications and mitigation strategies enable the ability to swiftly and effectively respond. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | **RS.CO-2, RS.CO-3, RS.CO-4** | RS.CO-1, RS.CO-5 |
| Mitigation | **RS.MI-2** | RS.MI-1, RS.MI-3 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Communications | RS.CO-1: Personnel know their roles and order of operations when a response is needed | ***Rationale only provided for High Priority Subcategories*** | * ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 * ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 * NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 | IR-3a, -5b |
| Communications | **RS.CO-2: Events are reported consistent with established criteria** | **Reporting offshore operations events that have been identified as cybersecurity-relevant maintains operational security by ensuring the necessary information is reported to the correct stakeholders in a timely manner so that a proper response can be initiated.**  **The selection of RS.CO-2 assumes RS.CO-1 is being addressed.** | * **ISA 62443-2-1:2009 4.3.4.5.5** * **ISO/IEC 27001:2013 A.6.1.3, A.16.1.2** * **NIST SP 800-53 Rev. 4  AU-6, IR-6, IR-8** | **IR-1a, -1b** |
| Communications | **RS.CO-3: Information is shared consistent with response plans** | **Communications and response plans should be coordinated to ensure all stakeholders understand the status of the operating environment, actions required of them, and when to perform those actions. Response plans may address whether and how to share information from monitoring tools, threat indicators and other pertinent information regarding a cybersecurity incident. In addition to sharing information with internal and external partners, response plans should address sharing information with law enforcement and information sharing environments when necessary and practicable.** | * **ISA 62443-2-1:2009 4.3.4.5.2** * **ISO/IEC 27001:2013 A.16.1.2** * **NIST SP 800-53 Rev. 4  CA-2, CA-7, CP-2, IR-4,  IR-8, PE-6, RA-5, SI-4** | **ISC-1a, -1b, -1c, -1d,**  **IR-3d, -3i, -3l** |
| Communications | **RS.CO-4: Coordination with stakeholders occurs consistent with response plans** | **Responding to a cybersecurity event takes coordination across multiple parts of the organization to ensure the right activities can be conducted at the right time. Response plans describe the minimum activities that must be coordinated between stakeholders for a successful response to a cybersecurity event. RS.CO-4 is the most important of the High Priority Subcategories in Respond for Mission Objective 7.** | * **ISA 62443-2-1:2009 4.3.4.5.5** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8** | **IR-3d, -5b** |
| Communications | RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | *Rationale only provided for High Priority Subcategories* | * NIST SP 800-53 Rev. 4  PM-15, SI-5 | ISC-1a, -1c, -1d, -1e,  -1f, -1h, -1i, -1j, -1k, -1l |

|  |  |  |
| --- | --- | --- |
| Recover | Reputation and public relations recovery are highly dependent upon effective stakeholder communications. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | **RC.CO-3** | RC.CO-1, RC.CO-2 |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Communications | RC.CO-1: Public relations are managed | ***Rationale only provided for High Priority Subcategories*** | • COBIT 5 EDM03.02 | RM-1c |
| Communications | RC.CO-2: Reputation after an event is repaired | ***Rationale only provided for High Priority Subcategories*** | • COBIT 5 MEA03.02 | IR-3d |
| Communications | **RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams** | **Communications are a critical component of executing the operational aspects of recovery plans. The operational aspects of recovery, covered under Mission Objectives 1, 2, and 4, are more important than managing reputation and public perception. However, recovery plans and implementing improvements intersect with consistent and effective stakeholder communications.** | * **NIST SP 800-53 Rev. 4 CP-2, IR-4** | **IR-3d** |

## **B-8 Mission Objective 8: Maintain Operational Efficiency**

|  |
| --- |
| ***Mission Objective 8: Maintain Operational Efficiency***  Ensuring offshore facility and vessel operations continue to function optimally. Promoting operational capabilities through: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, Access Control, Data Security, Information Protection Processes and Procedures, Maintenance, Improvements. Organizations should maintain standards that support tuning equipment for optimal performance. Organizations should:   * identify and manage assets and their relationships to business processes * identify and manage stakeholder roles, including third party roles, in efficient execution of business processes * protect business process integrity |

|  |  |  |
| --- | --- | --- |
| Identify | Asset management, business environment, risk assessment, and risk management strategy are the primary methods used to identify procedures, technologies, and equipment that support the organization’s ability to maintain operational efficiency of offshore operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM05** | ID.AM-6 |
| Business Environment | **ID.BE-1, ID.BE-3, ID.BE-4** | ID.BE-5 |
| Risk Assessment | **ID.RA-4, ID.RA-5, ID.RA-6** |  |
| Risk Management Strategy | **ID.RM-2** | ID.RM-3 |

| 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 offshore operations provides the foundation for identifying and prioritizing assets that are most critical to maintaining operational efficiency.** | * **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 software platforms and applications that support offshore operations is critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **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 are critical to ensuring the necessary activities are happening when and as intended. In the operational efficiency context, they not only apply to human communications and data flow, but also 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 or facility, external communications, such as those necessary to support GPS navigation, and intermittent or continuous communication and data flow between offshore 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-4: External information systems are catalogued** | **Offshore operations are diverse, including activities supported by multiple organizations and third-party assets. Understanding the interplay between information systems provides the information necessary to optimize the performance between systems and system components. Maintaining awareness of external information systems provides the foundation for identifying and prioritizing assets that are most critical to maintaining operational efficiency. Understanding external information systems that support offshore operations is also critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations.**  **In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **COBIT 5 APO02.02** * **ISO/IEC 27001:2013 A.11.2.6** * **NIST SP 800-53 Rev. 4 AC-20, SA-9** | **EDM-1a, -1c, -1e, -1g**  **RM-1c** | |
| 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 operational efficiency impacts to offshore operations resources are necessary factors to consider when prioritizing resources. For example, monitoring activities may slow performance of some systems. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. 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 | |
| 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 the offshore 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 offshore operations are most critical 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-3: Priorities for organizational mission, objectives, and activities are established and communicated** | **Effectively protecting offshore 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.**  **The selection of ID.BE-3 assumes ID.BE-1 and ID.BE-2 are being addressed.** | * **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 offshore 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, and 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 | *Rationale only provided for High Priority Subcategories* | * 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 | |
| Risk Assessment | **ID.RA-4: Potential business impacts and likelihoods are identified** | **Internal and external business impacts are factors to consider during risk assessments.**  **Internally, understanding business impacts influences specific controls selected to support objectives and how they are implemented. Business impacts take into account impacts to and from other third parties, including business partners, service providers, and other contractors, as well as supply chain impacts. This allows traceability from critical business and mission systems to system hardware, software, and firmware components.**  **Externally, business impacts may lead to broader critical infrastructure impacts. For example, severe business impacts to large organizations or supply chains could impact the availability of supplies and services and possibly the Nation’s economy.** | * **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 an offshore operating 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 operational efficiency needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect operational efficiency, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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 offshore 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. For risks that impact continuity and integrity of offshore operations, “accept” may only be an appropriate option under limited circumstances. 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** | |
| Risk Management Strategy | **ID.RM-2: Organizational risk tolerance is determined and clearly expressed** | **Some degree of risk will always exist in the offshore operations context.**  **Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame.[[12]](#footnote-12) Clear risk tolerance boundaries help define an acceptable level of activity to maximize efficiency in operations.** | * **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 | ***Rationale only provided for High Priority Subcategories*** | * NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 | RM-1b, -1c | |

|  |  |  |
| --- | --- | --- |
| Protect | Maintaining a state of operational efficiency requires effective access controls and data security measures in addition to well documented policies and procedures and adequate awareness and training activities. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-4, PR.AC-5** |  |
| Data Security | **PR.DS-2, PR.DS-4** | PR.DS-1 |
| Information Protection Processes & Procedures | **PR.IP-7, PR.IP-8** | PR.IP-1, PR.IP-5 |
| Maintenance | **PR.MA-1** | PR.MA-2 |

| 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 that 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** | **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 offshore operations. Network integrity is critical to ensuring 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** |
| Data Security | PR.DS-1: Data-at-rest is protected | *Rationale only provided for High Priority Subcategories* | * 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.**  **Offshore operations data at rest is generally harder to get to on offshore facilities and vessels than data in transit that may be traveling to another facility or vessel or onshore. PR.DS-1 is a Moderate Priority to reflect that data in transit carries more risk than data at rest in the offshore operations context.** | * **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** | **Capacity planning is conducted to identify and address threats to offshore operations. Maintaining adequate capacity ensures 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** |
| 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 and Procedures | PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | *Rationale only provided for High Priority Subcategories* | * 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-7: Protection processes are continuously improved** | **Regularly examining the effectiveness and efficiency of protection processes provides organizations with valuable feedback regarding how their cybersecurity efforts to protect offshore operations assets are performing, and where improvements need to be made over time as problems or improved practices are identified. Additionally, the threat environment for offshore operations may continue to evolve even when organizations do not make signification changes to their environment (e.g., new vulnerabilities for an existing technology may be discovered).** | * **COBIT 5 APO11.06, DSS04.05** * **ISA 62443-2-1:2009 4.4.3.1, 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 SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6** | **CPM-1g** |
| Information Protection Processes & Procedures | **PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties** | **Sharing authorized information regarding the effectiveness of protection technologies benefits organizations internally and the industry externally by reducing the collective level of effort in determining which cybersecurity resources are most effective. Organizations will need to determine the appropriate parties for sharing this information. Examples include business partners, supply chain partners, and threat intelligence sharing partners (e.g., FBI InfraGard or the Oil & Natural Gas Information Sharing and Analysis Center [ONG-ISAC]).** | * **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** |
| 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 offshore assets safeguards against preventable issues that could impact the efficiency of operations. 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.** | * **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 |

|  |  |  |
| --- | --- | --- |
| Detect | Operational efficiency relies on continuous monitoring to identify non-conformance with controls that may reduce optimal functionality of offshore operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-8** |  |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |

|  |  |  |
| --- | --- | --- |
| Respond | Operational efficiency relies on continual improvements based on lessons learned from operating the environment over time and responding to cybersecurity incidents. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Improvements | **RS.IM-1** | N/A |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Improvements | **RS.IM-1: Response plans incorporate lessons learned** | **Lessons learned from responding to a cybersecurity event provide valuable feedback for policy, procedural, and operational improvements that both prevent or reduce adverse impacts to offshore operations and aid the organization in evolving to optimize efficiencies over time.** | * **COBIT 5 BAI01.13** * **ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4** * **ISO/IEC 27001:2013 A.16.1.6** * **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8** | **IR-3h** |

|  |  |  |
| --- | --- | --- |
| 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 |

## **B-9 Mission Objective 9: Maintain Secure Communications**

|  |
| --- |
| ***Mission Objective 9: Maintain Secure Communications***  Ensuring communications required to operate positioning equipment and external communications are available reliably. Protecting communications channels through: Asset Management, Risk Assessment, Access Control, Data Security, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes. Organizations should:   * understand the facility’s or vessel’s external communication paths * protect integrity of positioning equipment and other equipment that can be adversely impacted via external communication paths * protect personal information * implement redundant systems, where appropriate, to limit the risk of communications loss |

|  |  |  |
| --- | --- | --- |
| Identify | Communications assets and other assets that may impact them must be identified and evaluated through the organizations risk assessment processes. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-3, ID.AM-4, ID.AM-5** | ID.AM-1, ID.AM-2 |
| Risk Assessment | **ID.RA-3, ID.RA-5** | ID.RA-1 |

| 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-3: Organizational communication and data flows are mapped** | **Understanding the flow of data and the communications channels for it are critical to ensuring the necessary activities are happening when and as intended. Secure communications support many aspects of offshore operations, from positioning systems to personal information. Consider frequent communications that are contained on the vessel or facility, external communications, such as those necessary to support GPS navigation, and intermittent communications, such as when a vessel arrives at port. All critical offshore operations activities that involve intermittent or continuous communication and data flow between offshore and onshore facilities should be protected.** | * **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-4: External information systems are catalogued** | **Offshore operations are diverse, including activities supported by multiple organizations and third-party assets. Understanding the interplay between information systems, internally and externally, provides the information necessary to secure communications between systems and system components. Maintaining awareness of external information systems provides the foundation for identifying and prioritizing assets that are most critical to maintaining secure communications. Understanding external information systems that support offshore operations is also critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **COBIT 5 APO02.02** * **ISO/IEC 27001:2013 A.11.2.6** * **NIST SP 800-53 Rev. 4 AC-20, SA-9** | **EDM-1a, -1c, -1e, -1g**  **RM-1c** | |
| 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 secure communications impacts to offshore operations resources are necessary factors to consider when prioritizing resources. For example, taking a communications system offline for maintenance during active operations may degrade the performance of positioning equipment. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. 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** | |
| 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 to operate secure communications helps organizations manage risks accordingly, and to plan for addressing potential incidents related to those specific threats if the risks associated with them are realized.**  **The selection of ID.RA-3 assumes ID.RA-1 is being addressed.** | * **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 communications technologies employed in an offshore operating 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 operational needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect secure communications, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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** |

|  |  |  |
| --- | --- | --- |
| Protect | Securing communications channels relies on strong access controls, data security practices, procedures and processes, and protective technologies to prevent issues such as data leaks and issues with navigation and positioning. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-1, PR.AC-4, PR.AC-5** | PR.AC-2, PR.AC-3 |
| Data Security | **PR.DS-1, PR.DS-2, PR.DS-5** | PR.DS-3 |
| Information Protection Processes and Procedures | **PR.IP-1, PR.IP-3, PR.IP-7, PR.IP-9** | PR.IP-11, PR.IP-12 |
| Protective Technology | **PR.PT-3, PR.PT-4** | PR.PT-2 |

| 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 assuring 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 | *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-3: Remote access is managed | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01, DSS01.04, DSS05.03 * ISA 62443-2-1:2009 4.3.3.6.6 * ISA 62443-3-3:2013 SR 1.13, SR 2.6 * ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 * NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 | 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 that have a need-to-know and have received proper training for completing their duties.**  **Communications channels must be carefully managed to ensure they are available when needed and that only the intended communications are being sent and received across the appropriate channels.**  **The selection of PR.AC-4 assumes PR.AC-2 and PR.AC-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 offshore operations. Network integrity is critical to ensuring 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** |
| 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 off-line 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** | **Communications must be protected as they travel across internal and external networks, particularly external networks where they 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-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 positioning, 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. Examples include causing confusion or other issues between business partners, a public relations challenge, loss of proprietary methods or drilling locations, or indicators of system health, depending on the circumstances surrounding a leak. 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** | **Validated and tested baseline configurations promote consistency when configuring new systems and enable secure communications. Baselines also support response and recovery efforts in returning to a desired operating state after an incident.** | * **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 each proposed change is carefully reviewed prior to approval to proceed. Following consistent methodologies supports secure communications 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 so as limit adverse impacts to offshore operations communications.** | * **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 & Procedures | **PR.IP-7: Protection processes are continuously improved** | **Regularly examining the effectiveness and efficiency of protection processes provides organizations with valuable feedback regarding how their cybersecurity efforts to protect offshore operations communications assets are performing, and where improvements need to be made over time as problems or improved practices are identified. Additionally, the threat environment for offshore operations communications may continue to evolve even when organizations do not make signification changes to their environment (e.g., new vulnerabilities for an existing technology may be discovered).** | * **COBIT 5 APO11.06, DSS04.05** * **ISA 62443-2-1:2009 4.4.3.1, 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 SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6** | **CPM-1g** |
| 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** | **Offshore operations response and recovery plans define the degree of security communications 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 they are periodically updated, allowing the organization to maintain an acceptable level of preparedness. This activity supports response and recovery activities so that offshore operations can return to a desirable state expediently. The selection of PR.IP-9 assumes PR.IP-10 is addressed. 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-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 |
| Information Protection Processes & Procedures | PR.IP-12: A vulnerability management plan is developed and implemented | *Rationale only provided for High Priority Subcategories* | * 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 |
| Protective Technology | PR.PT-2: Removable media is protected and its use restricted according to policy | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.02, APO13.01 * ISA 62443-3-3:2013 SR 2.3 * ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 * NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 | IAM-2a, -2b, -2c, -3e,  -3f |
| 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 limits access to resources to only those that have a need to access communications systems or 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 that 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 offshore operations 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 | Detecting issues with communications channels requires continuous monitoring of security controls and incident detection processes. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-1, DE.CM-6, DE.CM-7, DE.CM-8** |  |
| Detection Processes | **DE.DP-1** | DE.DP-3, DE.DP-4 |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| 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 offshore 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-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 secure communications and identify anomalies that can lead to cybersecurity events with adverse impacts.** | * **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 secure communications 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 offshore operations communications provide input into event correlation and analysis tools, alert mechanisms, and the response process.** | * **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** | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |
| Detection Processes | **DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability** | **Detection activities identify incidents that may impact offshore operations communications. Ensuring accountable individuals are assigned roles and responsibilities for detection activities increases the likelihood of performing these activities effectively. For example, assigning responsibility to look for signs of an incident when performing routine maintenance improves the likelihood of detecting an incident. Collaboration between points-of contact (POCs) is important. At a minimum, consider defining roles and responsibilities for critical POCs, such as rig POC, vendor POC, operator POC, drilling contractor POC and establishing the most critical roles and responsibilities for the organization first.** | * **CCS CSC 5** * **COBIT 5 DSS05.01** * **ISA 62443-2-1:2009 4.4.3.1** * **ISO/IEC 27001:2013 A.6.1.1** * **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14** | **WM-1a, -1d, -1f** | |
| Detection Processes | DE.DP-3: Detection processes are tested | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.02 * ISA 62443-2-1:2009 4.4.3.2 * ISA 62443-3-3:2013 SR 3.3 * ISO/IEC 27001:2013 A.14.2.8 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 | IR-3e, -3j | |
| Detection Processes | DE.DP-4: Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO12.06 * ISA 62443-2-1:2009 4.3.4.5.9 * ISA 62443-3-3:2013 SR 6.1 * ISO/IEC 27001:2013 A.16.1.2 * NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 | IR-1b, -3c, -3n,  ISC-1a, -1c, -1d, -1h,  -1j | |

|  |  |  |
| --- | --- | --- |
| 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** |

## **B-10 Mission Objective 10: Maintain Regulatory Compliance/Compliance with Regulatory Audits & Inspection Requirements**

|  |
| --- |
| ***Mission Objective 10: Maintain Regulatory Compliance/Compliance with Regulatory Audits & Inspection Requirements***  Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Business Environment, Governance, Risk Management Strategy, Awareness and Training, Information Protection Processes and Procedures, Maintenance, Security Continuous Monitoring. Organizations should:   * track regulatory activity and assess impacts to operations * incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures as well as facility and organizational management systems * develop on-going relationships with regulators * ensure foundational “cyber hygiene” activities are addressed as part of the overall risk management program * contribute to industry standards and best practices |

|  |  |  |
| --- | --- | --- |
| Identify | The business environment, governance practices, and risk management strategy shape the requirements organizations must meet to enable offshore operations. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-2, ID.BE-3** |  |
| Governance | **ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4** |  |
| Risk Management Strategy | **ID.RM-1, ID.RM-3** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Business Environment | **ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies energy systems, which includes the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[13]](#footnote-13) Each organization should understand its role as part of the critical infrastructure and ensure stakeholders understand their individual and collective roles in supporting critical infrastructure activities. Compliance activities are a starting point for strengthening the security posture of organizations and ensure they maintain the ability to operate.** | * **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** | **Effectively protecting offshore operations assets depends on stakeholder awareness of the organization’s mission, and objectives, and how those things influence their implementation of regulatory activities, both generally and specifically for properly managing and protecting the priority systems and assets of the organization. Priorities also influence the nature and frequency of training provided to ensure the systems and assets with operational priority remain in compliance and therefore operational.** | * **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** |
| Governance | **ID.GV-1: Organizational information security policy is established** | **Policies are the top-level, organization-specific implementation of regulatory requirements in organizations. They drive the processes, procedures, controls, and other activities of the organization, including those that directly and indirectly address cybersecurity needs. To ensure policies remain current and effective, they are reviewed periodically and updated as needed.** | * **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** | **Operating certain IT and OT equipment necessitates an adequate degree of knowledge and experience, which can be demonstrated through the achievement of licenses, certifications, and other professional designations. In some cases, a current license is a condition for operating OT equipment. These requirements must be considered when defining and assigning security roles and responsibilities. Similarly, licensing requirements should be considered when making implementation decisions regarding the access controls Subcategories (PR.AC). Coordination helps ensure all parties are aligning personnel with the appropriate roles and responsibilities to meet regulatory requirements across multi-organization teams.** | * **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 offshore operations activities may be driven or influenced by multiple laws, Executive Orders, directives, policies, and regulations, including internal organizational policies. Audits and inspections will be conducted against applicable drivers, including considerations for cybersecurity. Maintaining an acceptable state of audit or inspection readiness provides a reasonable foundation for addressing known risks, and also saves resources expended to prepare for and participate in audits and inspections.**  **Additionally, protecting workforce information from loss, theft, or other compromises ensures the organization can meet these requirements. Protecting workforce information also prevents harms to individuals, such as identity theft or embarrassment, and harms to the organization, such as diversion of resources away from operational objectives or employee distractions due to dealing with identify theft.**  **Policies and practices of organizations may vary. When working with third parties, a formal agreement that clearly describes expectations for information governance between all the parties should be executed.** | * **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, Executive Orders, 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 offshore operations regulatory requirements 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-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis** | **As discussed in Presidential Policy Directive (PPD) 21, the Nation's critical infrastructure provides the essential services that underpin American society. 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. PPD-21 identifies transportation systems, which includes parts of the oil & natural gas industry and its operations, as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors.[[14]](#footnote-14)**  **Risk management processes align the organizational risk tolerances with the priorities of internal and external stakeholders, including regulators.** | * **NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14** | **RM-1b, -1c** |

|  |  |  |
| --- | --- | --- |
| Protect | The ability to demonstrate a state of compliance relies heavily on well documented policies and procedures, adequate awareness and training activities, and periodic maintenance. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1** | PR.AT-3 |
| Information Protection Processes and Procedures | **PR.IP-1, PR.IP-5, PR.IP-8** | PR.IP-9, PR.IP-12 |
| Maintenance | **PR.MA-1** | PR.MA-2 |

| 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 regulatory compliance. In the context of regulatory compliance, stakeholders that make major decisions regarding offshore operations and those that interact with regulators (e.g., senior executives) must understand regulatory requirements and the commitments they are making on behalf of the organization.** | * **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, -3b, -3c, -3d,**  **-3g, -3h, -3i, -4a** |
| Awareness and Training | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * 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 |
| Information Protection Processes & Procedures | **PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained** | **Baselines are developed in accordance with regulatory requirements and the organization’s risk tolerance. 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.** | * **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-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** | **Sharing authorized information regarding the effectiveness of protection technologies benefits organizations internally and the industry externally by reducing the collective level of effort in determining which cybersecurity resources are most effective in meeting regulatory compliance obligations. Organizations will need to determine the appropriate parties for sharing this information. Examples include business partners, supply chain partners, and threat intelligence sharing partners (e.g., FBI InfraGard or the Oil & Natural Gas Information Sharing and Analysis Center [ONG-ISAC]).** | * **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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and  managed | *Rationale only provided for High Priority Subcategories* | * 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,  -5d, -5e, -5f, -5g, -5h,  -5i,  TVM-1d,  RM-1c |
| Information Protection Processes & Procedures | PR.IP-12: A vulnerability management plan is developed and implemented | *Rationale only provided for High Priority Subcategories* | * 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 |
| 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 offshore assets safeguards against preventable issues that could impact 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 |

|  |  |  |
| --- | --- | --- |
| Detect | Detection processes must comply with applicable rules and regulations. Security continuous monitoring helps ensure controls are operating as intended to support regulatory requirements. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-7, DE.CM-8** |  |
| Detection Processes |  | DE.DP-2 |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Security Continuous Monitoring | **DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed** | **Monitoring for unauthorized activities supports regulatory compliance 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 offshore operations provide input into event correlation and analysis tools, alert mechanisms, and the response process.** | * **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** | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |
| Detection Processes | DE.DP-2: Detection activities comply with all applicable requirements | *Rationale only provided for High Priority Subcategories* | * ISA 62443-2-1:2009 4.4.3.2 * ISO/IEC 27001:2013 A.18.1.4 * NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 | IR-1d, 5a, -1g, -5f,  TVM-1d,  RM-1c,  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 |

## **B-11 Mission Objective 11: Maintain Third Party Integration**

|  |
| --- |
| ***Mission Objective 11: Maintain Third Party Integration***  Protecting the supply chain and operating seamlessly in a multi-party environment, through: Asset Management, Business Environment, Governance, Risk Assessment, Access Control, and Awareness and Training. Organizations should:   * manage relationships with suppliers, vendors, contractors, consultants, and other entities that support operational and business activities * communicate requirements and assess their implementation throughout the supply chain * understand the interplay between personnel from all entities involved in operations |

|  |  |  |
| --- | --- | --- |
| Identify | Offshore operations rely on third party relationships that are supported by activities in asset management, business environment, governance, and risk assessment. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-3, ID.AM-4, ID.AM-5, ID.AM-6** |  |
| Business Environment | **ID.BE-1, ID.BE-4, ID.BE-5** | ID.BE-3 |
| Governance | **ID.GV-2, ID.GV-3** |  |
| Risk Assessment | **ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5** |  |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Asset Management | **ID.AM-3: Organizational communication and data flows are mapped** | **Understanding the flow of data and the communications channels for it are critical to ensuring the necessary activities are happening when and as intended. In the third-party integration context, they not only apply to human communications and data flow, but also communication and data flows for devices and equipment to support adequate monitoring so that issues that may lead to integration impacts are identified. Consider frequent communications that are contained on the vessel or facility, external communications, such as those necessary to support supplier relationships, and intermittent or continuous communication and data flow between offshore 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-4: External information systems are catalogued** | **Offshore operations are diverse, including activities supported by multiple organizations and third-party assets. Understanding the interplay between information systems, internally and externally, provides the information necessary to manage third party integration, including policies, processes, systems, and assets. Maintaining awareness of external information systems provides the foundation for identifying and prioritizing assets that are most critical to managing the operational aspects of integration. Understanding external information systems that support offshore operations is also critical to ensuring vessel and facility software is properly supported and that there is adequate visibility into operations. In the offshore operations context, this Subcategory is most relevant to systems on offshore facilities and vessels and any onshore systems that extend to offshore assets.** | * **COBIT 5 APO02.02** * **ISO/IEC 27001:2013 A.11.2.6** * **NIST SP 800-53 Rev. 4 AC-20, SA-9** | **EDM-1a, -1c, -1e, -1g**  **RM-1c** | |
| 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 third-party integration impacts to offshore operations resources are necessary factors to consider when prioritizing resources. For example, taking a system offline for maintenance during active operations may impede the ability of a business partner to function. Resource prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. 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 personnel to effectively carry out cybersecurity activities with third party counterparts. 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, such as rig POC, vendor POC, operator POC, drilling contractor POC, and establishing the most critical roles and responsibilities for the organization first.** | * **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** | |
| 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 the offshore 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 offshore operations are most critical 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-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 offshore operations activities required for third party integration. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated operational functions and activities, and traceability to specific assets for all parties involved in an operation.** | * **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 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** | |
| Governance | **ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners** | **Operating certain IT and OT equipment necessitates an adequate degree of knowledge and experience, which can be demonstrated through the achievement of licenses, certifications, and other professional designations. In some cases, a current license is a condition for operating OT equipment. These requirements must be considered when defining and assigning security roles and responsibilities. Similarly, licensing requirements should be considered when making implementation decisions regarding the access controls Subcategories (PR.AC). Coordination helps ensure all parties are aligning personnel with the appropriate roles and responsibilities to meet regulatory requirements across multi-organization teams. Certifications can indicate to business partners the level of competency key players have achieved.** | * **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 offshore operations activities may be driven or influenced by multiple laws, Executive Orders, directives, policies, and regulations, including internal organizational policies. Audits and inspections will be conducted against applicable drivers, including considerations for cybersecurity. Maintaining an acceptable state of compliance provides a reasonable foundation for addressing known risks, and also saves resources expended to prepare for and participate in audits and inspections.**  **Additionally, protecting workforce information from loss, theft, or other compromises ensures the organization can meet these requirements. Protecting workforce information also prevents harms to individuals, such as identity theft or embarrassment, and harms to the organization, such as diversion of resources away from operational objectives or employee distractions due to dealing with identify theft.**  **Policies and practices of organizations may vary, as may specific regulatory requirements. When working with third parties, a formal agreement that clearly describes expectations for all the parties should be executed.** | * **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** | |
| Risk Assessment | **ID.RA-1: Asset vulnerabilities are identified and documented** | **Cybersecurity vulnerabilities in offshore operations that are exploited can lead to unpredictable behaviors of control systems, including malfunctions that cause operations issues with varying degrees of severity. Identifying vulnerabilities for control systems assets, and understanding how those vulnerabilities may impact third party integration, is the starting point for conducting realistic risk assessments and determining appropriate risk responses.** | * **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-2: Threat and vulnerability information is received from information sharing forums and sources** | **Industry-specific sharing forums, such as FBI InfraGard special interest groups and the ONG-ISAC, provide a centralized mechanism for sharing threat and vulnerability information anonymously and for receiving aggregated information and analyses from others in industry about threats and vulnerabilities other organizations have not yet seen. Participation in these forums can elevate the security posture of the industry generally as well as individual organizations by helping all participants rapidly come up to speed on changing technologies and threats.** | * **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** * **ISO/IEC 27001:2013 A.6.1.4** * **NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5** | **TVM-1a, -1b, -2a, -2b** | |
| 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 third party integration risks accordingly, and to plan for addressing potential incidents related to those specific threats if the risks associated with them are realized.** | * **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** | **Internal and external business impacts are factors to consider during risk assessments.**  **Internally, understanding business impacts influences specific controls selected to support objectives and how they are implemented. Business impacts take into account impacts to and from third parties, including business partners, service providers, and other contractors, as well as supply chain impacts. This allows traceability from critical business and mission systems to system hardware, software, and firmware components.**  **Externally, business impacts may lead to broader critical infrastructure impacts. For example, severe business impacts to large organizations or supply chains could impact the availability of supplies and services or even the Nation’s economy.** | * **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 technologies employed in an offshore operating 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 operational needs. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect third party integration, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes across third parties must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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** |

|  |  |  |
| --- | --- | --- |
| Protect | Third party integration relies heavily on access controls and adequate awareness and training activities. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-4, PR.AC-5** |  |
| Awareness and Training | **PR.AT-1, PR.AT-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 or third-party relationships, 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 that have a need-to-know and have received proper training for completing their duties.** | * **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 offshore operations. Network integrity is critical to ensuring 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. Integration of networks between third parties will require additional protections and coordination.** | **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 third party integration training accountability. In the context of third party integration, stakeholders must understand the requirements of their own organization as well as those that may differ in the context of the third-party relationship.**  **The selection of PR.AT-1 assumes PR.AT-2 and PR.AT-4 are being addressed.** | * **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 offshore operations rely heavily on a diverse contractor base to function. All personnel on offshore facilities and vessels, 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 facility or 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** |

|  |  |  |
| --- | --- | --- |
| Detect | Detection processes rely on continuous monitoring activities that must be coordinated across third-party relationships, when applicable. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-8** | N/A |

| Detailed Specifications | | | Optional Resources | | |
| --- | --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |

|  |  |  |
| --- | --- | --- |
| 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 |

## **B-12 Mission Objective 12: Maintain Logistics**

|  |
| --- |
| ***Mission Objective 12: Maintain Logistics***  Managing the movement of personnel, equipment, and supplies that sustain operations, through: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, Data Security. Organizations should:   * know which personnel should be where and when, and whether personnel are at the proper location as expected (e.g., the right person is on the right facility or vessel at the right time) * know which transportation modalities are in operation and where they are located (e.g., boats, helicopters) * protect the physical security of personnel, equipment, and supplies from the point of origin to destination * ensure supplies that support operations are available when needed (e.g., personnel supplies, such as food, and operational supplies, such as spare parts and back up equipment) |

|  |  |  |
| --- | --- | --- |
| Identify | Protecting logistics requires activities in asset management, business environment, risk assessment, and risk management strategy to help ensure all people and assets are where they are needed when they are needed. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-1, ID.AM-5, ID.AM-6** | ID.AM-3 |
| Business Environment | **ID.BE-3, ID.BE-4, ID.BE-5** | ID.BE-1 |
| Risk Assessment | **ID.RA-4, ID.RA-5** | ID.RA-1, ID.RA-6 |
| Risk Management Strategy | **ID.RM-1** |  |

| 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 processes, people, assets, and supplies, as well as the physical devices and systems that support offshore operations logistics provides the foundation for identifying and prioritizing activities and systems that are most critical to maintaining logistics.** | * **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 | *Rationale only provided for High Priority Subcategories* | * 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 logistics impacts to offshore operations resources are necessary factors to consider when prioritizing processes, people, assets, supplies, devices, and systems. For example, taking a schedule management system offline for maintenance during active operations may impede the ability of the organization to determine which personnel are currently on a vessel when making weather evacuation preparations. Prioritization informs how Cybersecurity Framework Subcategories are addressed and which activities should be emphasized. Regular reviews and updates to prioritization based on changes to the operational environment 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** | |
| Business Environment | ID.BE-1: The organization’s role in the supply chain is identified and communicated | *Rationale only provided for High Priority Subcategories* | * 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-3: Priorities for organizational mission, objectives, and activities are established and communicated** | **Effectively protecting offshore operations logistics 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 processes, people, assets, supplies, devices, and systems of the operation.** | * **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 offshore operations activities required for logistics. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated operational functions and activities, and traceability to specific people, assets, supplies, devices, and systems.** | * **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** | **Stakeholders must coordinate to ensure critical logistical services and activities can continue operating in the event of an incident, even under adverse conditions in some instances. For example, maintaining a paper record of all personnel on a drilling platform in the event the personnel management system on board experiences an issue. 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** | |
| 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-4: Potential business impacts and likelihoods are identified** | **Internal and external business impacts are factors to consider during risk assessments.**  **Internally, understanding business impacts influences specific controls selected to support objectives and how they are implemented. Business impacts take into account impacts to and from third parties, including business partners, service providers, and other contractors, as well as supply chain impacts. This allows traceability from critical business and mission processes and systems to system hardware, software, and firmware components as well as people, assets, supplies, and devices.**  **Externally, business impacts may lead to broader critical infrastructure impacts. For example, severe business impacts to large organizations or supply chains could impact the availability of supplies and services or even the Nation’s economy.** | * **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 an offshore operating 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 logistics. Examining threats and vulnerabilities in the context of the organization’s operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect environmental safety, and also provides input into monitoring plans. Organizations that need help getting started with identifying threats and vulnerabilities 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. Roles, responsibilities, and processes must be established for identifying and qualifying risks as well as determining how to manage them once identified.**  **Note that approaches to handling vulnerabilities may necessarily 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** | **Addressing logistics risks during offshore 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** | |

|  |  |  |
| --- | --- | --- |
| Protect | Logistics rely heavily on adequate awareness and training and data security activities. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-5** |  |
| Data Security | **PR.DS-3, PR.DS-4** |  |

| Detailed Specifications | | | Optional Resources | |
| --- | --- | --- | --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Awareness and Training | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in offshore operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in cybersecurity 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, logistics personnel must understand how to prioritize responsibilities as needed.** | * **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** |
| Data Security | **PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition** | **Cybersecurity protections must be in place for assets throughout the full lifecycle of logistics. Inventories form the basis of information for managing these assets. Media assets are sanitized at the end of life using methods that are commensurate with the category or classification of information stored on them. Procedures are in place to control the entry and exit of assets and information. A record of asset removal, transfers, and dispositions is maintained.** | * **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 offshore operations. Maintaining adequate capacity ensures 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** |

|  |  |  |
| --- | --- | --- |
| Detect | Logistics depend on detection capabilities to identify anomalies and events, including through security continuous monitoring procedures. | |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events |  | DE.AE-2 |
| Security Continuous Monitoring | **DE.CM-8** |  |

| 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 | |
| Security Continuous Monitoring | **DE.CM-8: Vulnerability scans are performed** | **There are significant distinctions between IT and OT regarding whether and how this activity is conducted.**  **Conducting vulnerability scans on OT can be dangerous and should be prohibited in many cases. Doing so may consume all of a system’s resources and take the entire system down as a result. For example, simple ping requests have shut down process controls systems.**  **For IT systems, however, vulnerability scanning proactively identifies weaknesses in systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during offshore operations, including cybersecurity events that impact personnel safety. When it is not safe to conduct a vulnerability scan on an IT system, there may be more readily available alternatives than there are for OT systems, such as creating a mirror of the system to scan.** | * **COBIT 5 BAI03.10** * **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** * **ISO/IEC 27001:2013 A.12.6.1** * **NIST SP 800-53 Rev. 4 RA-5** | | **TVM-2e, -2i, -2j, -2k,**  **RM-1c** | |

|  |  |  |
| --- | --- | --- |
| 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. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-3)
4. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, “Risk Response Strategies” [↑](#footnote-ref-4)
5. 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-5)
6. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-6)
7. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, “Risk Response Strategies” [↑](#footnote-ref-7)
8. 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-8)
9. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-9)
10. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, “Risk Response Strategies” [↑](#footnote-ref-10)
11. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-11)
12. NIST SP 800-39, Managing Information Security Risk, Section 2.3.3 [↑](#footnote-ref-12)
13. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-13)
14. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience (February 12, 2103) [↑](#footnote-ref-14)