# **Maritime Bulk Liquids Transfer Profile**

This MBLT CFP defines the desired minimum state of cybersecurity by identifying the minimum set of Cybersecurity Framework Categories and Subcategories for each of the eight Mission Objectives required to conduct MBLT operations in a more secure manner. Appendix A is divided into a subsection for each of the eight Mission Objectives listed in Section 6.1, Table 6-1 of the profile overview document. Each Mission Objective subsection in Appendix A includes both a summary and detailed table of High and Moderate Priority Subcategory specifications in the Profile by Cybersecurity Framework Function and Category. Figure A-1 provides a legend that describes the layout of the detailed Profile content provided.

Figure A‑1. Appendix A Content Legend

****

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

|  |
| --- |
| ***Mission Objective 1: Maintain Personnel Safety***Cybersecurity-effect on process control systems impacts personnel safety. Organizations should:* manage risks to the organization and industry using a structured process
* identify and train personnel on interdependence of cybersecurity with operational responsibilities
* implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel safety
 |

|  |  |
| --- | --- |
| Identify | Risk assessments 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. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Risk Assessment | **ID.RA-1**, **ID.RA-5**, **ID.RA-6** | ID.RA-2, ID.RA-3, ID.RA-4 |
| Risk Management Strategy | **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 |
| Risk Assessment | **ID.RA-1: Asset vulnerabilities are identified and documented** | **Cybersecurity vulnerabilities in MBLT operations that are exploited can lead to unpredictable behaviors of control systems, including malfunctions that cause personnel safety issues ranging from minor harms to death. Identifying vulnerabilities for control systems assets, and understanding how those vulnerabilities may impact personnel safety, 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 | *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 the organization’s operating environment for MBLT operations, 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. Examining threats and vulnerabilities in the context of the organization’s particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.** | * **COBIT 5 APO12.02**
* **ISO/IEC 27001:2013 A.12.6.1**
* **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**
 | **RM-1c, -2j,** **TVM-2m** |
| Risk Assessment | **ID.RA-6: Risk responses are identified and prioritized** | **In order to protect personnel safety during maritime bulk liquid transport 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)** | * **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 MBLT 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-2a, -2b, -1a, -1b,** **-2c, -2d, -2e, 2g, -3a,** **-3b, -3c, -3d, -1c, -1d,** **-1e, -2h, -2j, -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 | Access control, 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 | N/A | PR.AC-5 |
| Awareness and Training | **PR.AT-5** | PR.AT-1, PR.AT-4 |
| Maintenance | N/A | 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-5: Network integrity is protected, incorporating network segregation where appropriate | *Rationale only provided for High Priority Subcategories* | * 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 | *Rationale only provided for High Priority Subcategories* | * 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-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Awareness and Training | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in MBLT operations must understand the policies and procedures 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, 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** |
| 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 |

|  |  |
| --- | --- |
| Detect | Real time awareness of monitoring systems, alerts is critical to personnel safety |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Security Continuous Monitoring | **DE.CM-2**, **DE.CM-8** | DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-7 |

|  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 | *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**  | **Monitoring facilities and physical equipment, devices, systems, and other assets for access issues and other activities is one of the primary ways anomalies can lead to cybersecurity events that impact personnel safety are identified.** | * **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** | **Vulnerability scanning proactively identifies weaknesses in IT or OT systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during MBLT operations, including cybersecurity events that impact personnel safety.** | * **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 | Proper response and communication plan development and utilization is critical in the response phase of maintaining personnel safety |
| --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Response Planning | N/A | RS.RP-1 |
| Communications | **RS.CO-1**, **RS.CO-4** | RS.CO-2, RS.CO-3 |

| 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 | *Rationale only provided for High Priority Subcategories* | * 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, IR8
 | 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-2: Events are reported consistent with established criteria | *Rationale only provided for High Priority Subcategories* | * 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, IR-1b |
| Communications | RS.CO-3: Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* | * 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, IR4, 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 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** |

| Recover | Recovery plan development and utilization are critical to the recovery phase of maintaining personnel safety |
| --- | --- |
| Categories | High Priority Subcategories | Moderate Priority Subcategories |
| Recovery Planning | N/A | 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 | *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 |

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

|  |
| --- |
| ***Mission Objective 2: Maintain Environmental Safety***Cybersecurity-effect on process control systems impacts environmental safety. Organizations should:* manage risks to the organization and industry using a structured process
* identify and train personnel on interdependence of cybersecurity with operational responsibilities
* manage prominent and increasing role of automated systems in maintaining quality control of product during safe transport
* implement Detect/Respond/Remediate activities where cybersecurity adversely affects environmental safety
 |

|  |  |
| --- | --- |
| Identify | Asset management and risk assessment were seen as the most significant Categories in the Identify functional area of the Cybersecurity Framework. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-1**, **ID.AM-5** | ID.AM-2 |
| Risk Assessment | N/A | ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Asset Management | **ID.AM-1: Physical devices and systems within the organization are inventoried** | **Maintaining a current inventory of the physical devices and systems that support MBLT operations provides the foundation for identifying and prioritizing assets that have environmental safety impacts.** | * **CCS CSC 1**
* **COBIT 5 BAI09.01, BAI09.02**
* **ISA 62443-2-1:2009 4.2.3.4**
* **ISA 62443-3-3:2013 SR 7.8**
* **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2**
* **NIST SP 800-53 Rev. 4 CM-8**
 | **ACM-1a, -1c, -1e, -1f** |
| Asset Management | ID.AM-2: Software platforms and applications within the organization are inventoried | *Rationale only provided for High Priority Subcategories* | * CCS CSC 2
* COBIT 5 BAI09.01, BAI09.02, BAI09.05
* ISA 62443-2-1:2009 4.2.3.4
* ISA 62443-3-3:2013 SR 7.8
* ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
* NIST SP 800-53 Rev. 4 CM-8
 | ACM-1a, -1c, -1e, -1f |
| Asset Management | **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value** | **Potential environmental safety impacts of MBLT operations resources are necessary factors to consider when prioritizing resources. Resource prioritization informs how Cybersecurity Framework functions are performed 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** |
| 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
 | TVM-2a, -2b, -2d, -2e, -2f, -2i, -2j, -2k, -2l, -2m |
| 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 | *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 | *Rationale only provided for High Priority Subcategories* | * 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 | Training, good maintenance programs and proper deployment of protective technology are critical to maintaining environmental safety |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | N/A | PR.AT-1, PR.AT-3, PR.AT-4, PR.AT-5 |
| Maintenance | N/A | PR.MA-1, PR.MA-2 |
| Protective Technology | **PR.PT-4** | PR.PT-1 |

| 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 | *Rationale only provided for High Priority Subcategories* | * 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 | *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 |
| Awareness and Training | PR.AT-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Awareness and Training | PR.AT-5: Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| 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-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | *Rationale only provided for High Priority Subcategories* | * CCS CSC 14
* COBIT 5 APO11.04
* ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
* ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
* NIST SP 800-53 Rev. 4 AU Family
 | SA-1a, -2a, -1b, -1c, -2e, -4a, -1d, -1e, -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 MBLT operations assets. This access is capable of providing 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 environmental safety 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 | Early detection of anomalies and events is critical to maintaining environmental safety |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | N/A | DE.AE-4, DE.AE-5 |

|  Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| 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-1d, RM-2j |

|  |  |
| --- | --- |
| Respond | Proper response and communication plan development and utilization is critical in the response phase of maintaining environmental safety |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Response Planning | N/A | 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 | *Rationale only provided for High Priority Subcategories* | * 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, IR8
 | **IR-3d** |

|  |  |
| --- | --- |
| Recover | Proper recovery planning is critical to mitigations when maintaining environmental safety |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Recovery Planning | N/A | 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 | *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 |

## **A-3 Mission Objective 3: Maintain Operational Security**

|  |
| --- |
| ***Mission Objective 3: Maintain Operational Security***Cybersecurity-effect on security control systems impacts operational safety and security. Organizations should:* manage risks to the organization and industry using a structured process
* identify and train personnel on interdependence of cybersecurity with operational responsibilities
* manage prominent and increasing role of automated systems in maintaining physical control of infrastructure
* implement Detect/Respond/Remediate activities where cybersecurity adversely affects safety and security
 |

|  |  |
| --- | --- |
| Identify | Proper risk assessment is critical to maintaining operational security |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Risk Assessment | **ID.RA-5** | ID.RA-1 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* | * CCS CSC 4
* COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
* ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
* ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
* NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
 | TVM-2a, -2b, -2d, -2e, -2f, -2i, -2j, -2k, -2l, -2m, RM-1c, -2j  |
| Risk Assessment | **ID.RA-5: Threats, vulnerabilities, likelihood, and impacts are used to determine risk** | **Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in the organization’s operating environment for MBLT operations 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. 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 operational security, and also provides input into monitoring plans.** | * **COBIT 5 APO12.02**
* **ISO/IEC 27001:2013 A.12.6.1**
* **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**
 | **RM-1c, -2j,** **TVM-2m** |

|  |  |
| --- | --- |
| Protect | Proper risk assessment is critical to maintaining operational security |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | **PR.AC-2** | PR.AC-1, PR.AC-4, PR.AC-5 |
| Awareness and Training | **PR.AT-5** | PR.AT-1, PR.AT-4 |
| Information Protection Processes & Procedures | **PR.IP-7**, **PR.IP-10**, **PR.IP-11** | PR.IP-1, PR.IP-4, PR.IP-5 |
| Maintenance | **PR.MA-1** | PR.MA-2 |
| Protective Technology | **PR.PT-4** | PR.PT-1, PR.PT-3 |

| 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 MBLT 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.** | * **COBIT 5 DSS01.04, DSS05.05**
* **ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8**
* **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3**
* **NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9**
 | **IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g** |
| Access Control | PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties | *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 |
| Access Control | PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | *Rationale only provided for High Priority Subcategories* | * 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, -3c, -3d |
| Awareness and Training | PR.AT-1: All users are informed and trained | *Rationale only provided for High Priority Subcategories* | * 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, -4a |
| Awareness and Training | PR.AT-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Awareness and Training | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in operational security 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, 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** |
| Information Protection Processes & Procedures | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained | *Rationale only provided for High Priority Subcategories* | * CCS CSC 3, 10
* COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
* ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
* ISA 62443-3-3:2013 SR 7.6
* ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
* NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
 | ACM-2a, -2b, -2c, -2d, -2e |
| Information Protection Processes & Procedures | PR.IP-4: Backups of information are conducted, maintained, and tested periodically | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.01
* ISA 62443-2-1:2009 4.3.4.3.9
* ISA 62443-3-3:2013 SR 7.3, SR 7.4
* ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
* NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
 | IR-4a, -4b |
| Information Protection Processes & Procedures | PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | *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 MBLT 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 MBLT operations may continue to evolve even when organizations do not make signification changes to IT and OT assets (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-10: Response and recovery plans are tested** | **Periodically testing response and recovery plans for MBLT operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization’s chances of more effectively restoring operational security efficiently and effectively.** | * **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11**
* **ISA 62443-3-3:2013 SR 3.3**
* **ISO/IEC 27001:2013 A.17.1.3**
* **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14**
 | **IR-3e, -4f, -3k, -4i, -4j** |
| Information Protection Processes & Procedures | **PR.IP-11: Cybersecurity is included in human resource practices (e.g. deprovisioning, personnel screening)** | **MBLT operations rely on personnel to operate and maintain IT and OT assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right access at the right times through activities, such as: screening personnel against applicable safety and knowledge conditions, provisioning and deprovisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.** | * **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05**
* **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3**
* **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4**
* **NIST SP 800-53 Rev. 4 PS Family**
 | **WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h** |
| 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 MBLT assets safeguards against preventable issues that could impact operational safety. 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, -2f, -2g, -2h |
| Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | *Rationale only provided for High Priority Subcategories* | * CCS CSC 14
* COBIT 5 APO11.04
* ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
* ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
* NIST SP 800-53 Rev. 4 AU Family
 | SA-1a, -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 | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.02
* ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
* ISO/IEC 27001:2013 A.9.1.2
* NIST SP 800-53 Rev. 4 AC-3, CM-7
 | IAM-2a, -2b, 2c, -2d, -2e, -2f, -2g, -2h, -2i |
| Protective Technology | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing 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 | Having robust detection processes which continuously monitor sensors and alarms for anomalies and events are critical to maintaining operational safety. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-1** | DE.AE-2, DE.AE-5 |
| Security Continuous Monitoring | **DE.CM-7** | DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-6, DE.CM-8 |
| Detection Processes | **DE.DP-2** | DE.DP-1, DE.DP-2, DE-DP-3, 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 MBLT 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, -2l, 3h |
| 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, TVM-1d, SA-2d, 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-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-6: External service provider activity is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* | * 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, SA9, 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 MBLT 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 | *Rationale only provided for High Priority Subcategories* | * 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-2: Detection activities comply with all applicable requirements** | **Monitoring and other detection activities that support operational security must be conducted in accordance with federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies, that apply to MBLT operations. Failing to comply with applicable requirements may result in issues such as gaps in detection activities, challenges pursuing sanctions, or legal action when warranted.** | * **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, -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-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 | Proper communications channels and procedures are key to response to an operational security incident |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | **RS.CO-2** | RS.CO-1RS.CO-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 MBLT operations events that have been identified as cybersecurity-relevant maintains operational security by ensuring the necessary information is reported to the correct entities in a timely manner so that a proper response can be initiated.** | * **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 | *Rationale only provided for High Priority Subcategories* | * 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, IR4, IR-8, PE-6, RA-5, SI-4
 | ISC-1a, -1b, -1c, -1d, IR-3d, -3i, -3l |

|  |  |
| --- | --- |
| Recover | Proper recovery planning is critical to maintaining operational security |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Recovery Planning | N/A | 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 | *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 |

## **A-4 Mission Objective 4: Maintain Preparedness**

|  |
| --- |
| ***Mission Objective 4: Maintain Preparedness***Cybersecurity-effect on systems readiness that can impact operations including maintenance, documentation and testing for safety and security. Organizations should:* develop systems and train personnel to integrate cybersecurity-impacts on resilience in maintaining mission assurance
* implement resilience-aware activities including
	+ risk mitigation procedures
	+ ongoing situational awareness
	+ backup/resilience/fail-safe modes
	+ regular preventive maintenance
 |

|  |  |
| --- | --- |
| Identify | Risk assessment is key to proper identification of risks in the maintain preparedness Mission Objective |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Risk Assessment | **ID.RA-5** | ID.RA-1 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* | * CCS CSC 4
* COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
* ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
* ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
* NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
 | TVM-1a, -1b, -2a, -2b, -2d |
| 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 the organization’s operating environment for MBLT operations 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. 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 the organization’s ability to maintain preparedness and also provides input into monitoring plans.** | * **COBIT 5 APO12.02**
* **ISO/IEC 27001:2013 A.12.6.1**
* **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**
 | **RM-1c, -2j,** **TVM-2m** |

|  |  |
| --- | --- |
| Protect | Proper training, planning & processes, maintenance and communications are key to maintaining preparedness |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-5** | PR.AT-1, PR.AT-4 |
| Information Protection Processes & Procedures | **PR.IP-9** | PR.IP-1, PR.IP-4, PR.IP-5, PR.IP-10, PR.IP-11, PR.IP-12 |
| Maintenance | **PR.MA-1** | PR.MA-2 |
| Protective Technology | **PR.PT-4** | PR.PT-1, PR.PT-3 |

| 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 | *Rationale only provided for High Priority Subcategories* | * 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-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, i1c, -1d, -1e, -1f, -1g |
| Awareness and Training | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in issues with maintaining preparedness 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, personnel must have an understanding of 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 |
| Information Protection Processes and 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-4: Backups of information are conducted, maintained, and tested periodically | *Rationale only provided for High Priority Subcategories* | * 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** | **MBLT 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.** | * **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 |
| Information Protection Processes and 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 and 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 MBLT assets safeguards against preventable issues that could impact the organization’s ability to maintain an acceptable level of preparedness. 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 software, 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-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | *Rationale only provided for High Priority Subcategories* | * CCS CSC 14
* COBIT 5 APO11.04
* ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
* ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
* NIST SP 800-53 Rev. 4 AU Family
 | SA-1a, -1b, -1c, -1d, -1e, -2a, -2e, -3d, -4a, -4f, -4g |
| Protective Technology | PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.02
* ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
* ISO/IEC 27001:2013 A.9.1.2
* NIST SP 800-53 Rev. 4 AC-3, CM-7
 | IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h, -2i |
| Protective Technology | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing 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 preparedness 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 must comply with applicable rules and regulations |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Detection Processes | **DE.DP-2** | DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| 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-2: Detection activities comply with all applicable requirements** | **Monitoring and other detection activities that support the ability to maintain an acceptable level of preparedness must be conducted in accordance with federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies, that apply to MBLT operations. Failing to comply with applicable requirements may result in issues such as gaps in detection activities, challenges pursuing sanctions, or legal action when warranted.** | * **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-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 plans that are property designed, built to, approved, inspected and trained for are key to maintaining preparedness. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Response Planning | N/A | RS.RP-1 |
| Communications | **RS.CO-2** | RS.CO-1, RS.CO-3 |

| 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 | *Rationale only provided for High Priority Subcategories* | * 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, IR8
 | IR-3d |
| 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-3d |
| Communications | **RS.CO-2: Events are reported consistent with established criteria** | **Reporting MBLT operations events that have been identified as cybersecurity-relevant helps organizations maintain an acceptable level of preparedness by ensuring the necessary information is reported to the correct entities in a timely manner so that a proper response can be initiated.** | * **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-3d** |
| Communications | RS.CO-3: Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* | * 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, IR4, IR-8, PE-6, RA-5, SI-4
 | IR-3d |

|  |  |
| --- | --- |
| Recover | Recovery planning and adapting capabilities based on field experience are key to maintaining preparedness. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Recovery Planning | N/A | RC.RP-1 |
| Improvements | N/A | RC.IM-1, RC.IM-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 |
| Improvements | RC.IM-1: Recovery plans incorporate lessons learned | *Rationale only provided for High Priority Subcategories* | * COBIT 5 BAI05.07
* ISA 62443-2-1:2009 4.4.3.4
* NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
 | IR-3h, -4i, -3k |
| Improvements | RC.IM-2: Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* | * COBIT 5 BAI07.08
* NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
 | IR-3h, -3k |

## **A-5 Mission Objective 5: Maintain Quality of Product**

|  |
| --- |
| ***Mission Objective 5: Maintain Quality of Product***Cybersecurity-effect on systems can impact product quality, maintenance, and systems monitoring. Impacts can include loss of confidentiality and integrity such as disclosure of status information or test results to unintended parties. Organizations should:* develop systems and train personnel to acknowledge potential cybersecurity risk vectors in maintaining product quality
* plan for quality measures including:
	+ testing
	+ preventive maintenance
	+ remediation
	+ ongoing situational awareness
* manage prominent and increasing role of automated systems in maintaining control of product during safe transport.
 |

|  |  |
| --- | --- |
| Identify | Assessing risks and understanding parameters about product are important to maintain product quality. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Asset Management | **ID.AM-5** | ID.AM-1, ID.AM-3, ID.AM-6 |
| Risk Assessment | **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-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** | **Potential product quality impacts of MBLT operations resources are necessary factors to consider when prioritizing resources. Resource prioritization informs how Cybersecurity Framework functions are performed with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.** | * **COBIT 5 APO03.03, APO03.04, BAI09.02**
* **ISA 62443-2-1:2009 4.2.3.6**
* **ISO/IEC 27001:2013 A.8.2.1**
* **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14**
 | **ACM-1a, -1b, -1c, -1d** |
| Asset Management | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO01.02, DSS06.03
* ISA 62443-2-1:2009 4.3.2.3.3
* ISO/IEC 27001:2013 A.6.1.1
* NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
 | WM-1a, -1b, -1c |
| Risk 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
 | TVM-2a, 2b, -2d, -2e, -2f, 2i, -2j, -2k, -2l, -2m, RM-1c, -2j |
| Risk Assessment | **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | **Understanding threats and vulnerabilities related to specific IT and OT technologies employed in the organization’s operating environment for MBLT operations, 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. 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 the organization’s ability to maintain product quality, and also provides input into monitoring plans.** | * **COBIT 5 APO12.02**
* **ISO/IEC 27001:2013 A.12.6.1**
* **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**
 | **RM-1c, 2j,** **TVM-2m** |

|  |  |
| --- | --- |
| Protect | Appropriate physical and information security requires training and technology to protect the product. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-5** | PR.AT-1, PR.AT-3 |
| Protective Technology | **PR.PT-4** | PR.PT-1, PR.PT-3 |

| 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 | *Rationale only provided for High Priority Subcategories* | * 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 | *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 |
| Awareness and Training | **PR.AT-5: Physical and information security personnel understand roles & responsibilities** | **Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in issues with maintaining product quality 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, personnel must have an understanding of 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** |
| Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | *Rationale only provided for High Priority Subcategories* | * CCS CSC 14
* COBIT 5 APO11.04
* ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
* ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
* NIST SP 800-53 Rev. 4 AU Family
 | SA-1a, -1b, -1c, -2a, -2e, -3d, -4e, -4f, -4g  |
| Protective Technology | PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS05.02
* ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
* ISO/IEC 27001:2013 A.9.1.2
* NIST SP 800-53 Rev. 4 AC-3, CM-7
 | IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h, -2i |
| Protective Technology | **PR.PT-4: Communications and control networks are protected** | **Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing 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 product quality 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 anomalies and events is critical to maintaining quality of bulk liquid products. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-2** | DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-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 | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS03.01
* ISA 62443-2-1:2009 4.4.3.3
* NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
 | SA-2a |
| Anomalies and Events | **DE.AE-2: Detected events are analyzed to understand attack targets and methods** | **Determining whether and how MBLT operational components are attacked provides insight into operational impacts that may affect the organization’s ability to maintain product quality.** | * **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 | *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, -2j, TVM-1d |
| 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, TVM-1d, SA-2d, RM-2j |

|  |  |
| --- | --- |
| Respond | Appropriate response planning is critical to maintain quality of bulk liquid products. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Response Planning | N/A | 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 | *Rationale only provided for High Priority Subcategories* | * 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, IR8
 | IR-3d |

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

## **A-6 Mission Objective 6: Meet HR Requirements**

|  |
| --- |
| ***Mission Objective 6: Meet HR Requirements***Cybersecurity-effect (security and privacy) on operational systems impacting security and trust of personnel and their information. Organizations should:* ensure appropriate governance, plans, procedures and oversight of connected HR systems and data including roles of employee managers in training and awareness
* understand risks, identify and train personnel on interdependence of cybersecurity with operational responsibilities and connections to source HR systems
* implement procedures to protect data in systems that contain personnel information
* implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel or personnel data.
 |

|  |  |
| --- | --- |
| Identify | HR requirements are closely aligned to governance requirements. Managing the workforce requires an understanding of internal and external security obligations. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Governance | **ID.GV-2, ID.GV-3** | ID.GV-1 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Governance | ID.GV-1: Organizational information security policy is established | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO01.03, EDM01.01, EDM01.02
* ISA 62443-2-1:2009 4.3.2.6
* ISO/IEC 27001:2013 A.5.1.1
* NIST SP 800-53 Rev. 4 -1 controls from all families
 | CPM-2g, -5d, RM-3e |
| Governance | **ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners** | **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, the associated access controls related Subcategories should be determined by the authorizations appropriate to the licensing level.**  | * **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 MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies, that govern information about the workforce that is collected and maintained by the organization. Protecting workforce information from loss, theft, or other compromises ensures the organization can meet HR 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.** | * **COBIT 5 MEA03.01, MEA03.04**
* **ISA 62443-2-1:2009 4.4.3.7**
 | **CPM-2k, IR-3n,** **RM-3f, -5f,****AACM-4f,** **IAM-3f,** **TVM-3f,** **SA-4f,** **ISC-2f,** **EDM-3f,** **WM-5f** |

|  |  |
| --- | --- |
| Protect | Personnel are often the first or second line of defense for the organization’s resources. Aligning cybersecurity requirements to HR activities aids the organization in achieving compliance with internal policies and procedures, including completion of training requirements maintaining appropriate levels of access to resources. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Awareness and Training | **PR.AT-1** | PR.AT-4, PR.AT-5 |
| Information Protection Processes & Procedures | **PR.IP-11** | PR.IP-1, PR.IP-4, PR.IP-5, PR.IP-9, PR.IP-10, PR.IP-12 |

| 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 MBLT operations.** | * **CCS CSC 9**
* **COBIT 5 APO07.03, BAI05.07**
* **ISA 62443-2-1:2009 4.3.2.4.2**
* **ISO/IEC 27001:2013 A.7.2.2**
* **NIST SP 800-53 Rev. 4 AT-2, PM-13**
 | WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i |
|  | PR.AT-2: Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.02, DSS06.03
* ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3
* 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 |
|  | 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 |
| Awareness and Training | PR.AT-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Information Protection Processes & Procedures | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained | *Rationale only provided for High Priority Subcategories* | * CCS CSC 3, 10
* COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
* ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
* ISA 62443-3-3:2013 SR 7.6
* ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
* NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
 | ACM-2a, -2b, -2c, -2d, -2e |
| Information Protection Processes & Procedures | PR.IP-4: Backups of information are conducted, maintained, and tested periodically | *Rationale only provided for High Priority Subcategories* | * 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.17.1.2, A.17.1.3, A.18.1.3
* NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
 | PR-4a, -4b |
| Information Protection Processes & 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, -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 | *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-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 |
| Information Protection Processes & Procedures | **PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** | **MBLT 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.** | * **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 |

|  |  |
| --- | --- |
| Detect | HR activities provide useful inputs for detecting anomalies and events. Conversely, understanding the HR context behind anomalies and events aids in determining potential and actual impacts of events. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Anomalies and Events | **DE.AE-2** | DE.AE-1, DE.AE-4, DE.AE-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 | *Rationale only provided for High Priority Subcategories* | * COBIT 5 DSS03.01
* ISA 62443-2-1:2009 4.4.3.3
* NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
 | SA-2a |
| Anomalies and Events | **DE.AE-2: Detected events are analyzed to understand attack targets and methods** | **Determining whether and how MBLT HR components are attacked provides insight into impacts that may affect the organization’s ability to maintain HR requirements.** | * **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-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 |

|  |  |
| --- | --- |
| Respond | Response capabilities help limit the impacts of a cybersecurity event on HR activities.  |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | **RS.CO-2** | RS.CO-3 |
| Mitigation | **RS.MI-3** | RS.MI-1, RS.MI-2 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Communications | RC.CO-2: Events are reported consistent with established criteria | *Rationale only provided for High Priority Subcategories* | * 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 | *Rationale only provided for High Priority Subcategories* | * 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, IR4, IR-8, PE-6, RA-5, SI-4
 | ISC-1a, 1b, -1c, -d, IR-3d, -3i, -3l |
| Mitigation | RS.MI-1: Incidents are contained | *Rationale only provided for High Priority Subcategories* | * 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-3b |
| Mitigation | RS.MI-2: Incidents are mitigated | *Rationale only provided for High Priority Subcategories* | * 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 |
| Mitigation | **RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks** | **When vulnerabilities that affect the organization’s ability to meet HR requirements are discovered in the process of responding to a cybersecurity event, organizations must determine the most effective risk response based on known information about the vulnerabilities that led to the event. Depending on the severity of a vulnerably that impacts HR requirements and the cybersecurity events it can lead to, acceptance may not be an appropriate response. Decisions made for short-term event response may not be the long-term risk response once the organization is in the Recover phase.** | * **ISO/IEC 27001:2013 A.12.6.1**
* **NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5**
 | **TVM-2c, -2f, -2g,** **-2m, -2n,** **RM-2j** |

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

## **A-7 Mission Objective 7: Pass Required Audits/Inspections**

|  |
| --- |
| ***Mission Objective 7: Pass Required Audits/Inspections***Developing systems and training personnel to demonstrate readiness and execution of established plans. Organizations should:* review plans and conduct in-person inspections via various means including:
	+ automated/cybersecurity interface testing
	+ sensor testing
	+ backup/resilience process evaluation
	+ plan and testing of data exchange/reporting methods
* ensure confidentiality of sensitive data, plans, and procedures
 |

|  |  |
| --- | --- |
| Identify | The business environment and governance practices shape the requirements organizations must meet order to pass required audits and inspections. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-5** | ID.BE-3, ID.BE-4 |
| Governance | **ID.GV-3** | ID.GV-4 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Business Environment | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | *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-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 |
| Business Environment | **ID.BE-5: Resilience requirements to support delivery of critical services are established** | **The ability to pass audits and inspections is contingent upon the IT and OT systems that support MBLT operations running at an acceptable capacity with adequate controls, even after a cybersecurity event occurs. Establishing what is acceptable and adequate for the organization requires advanced planning and coordination with relevant stakeholders.** | * **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-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed** | **Various MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, 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.** | * **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)**
 | **CPM-2k,** **IR-3n,** **RM-3f,** **AACM-4f,** **IAM-3f,** **TVM-3f,** **SA-4f,** **ISC-2f,** **IR-5f,** **EDM-3f,** **WM-5f** |
| Governance | ID.GV-4: Governance and risk management processes address cybersecurity risks | *Rationale only provided for High Priority Subcategories* | * 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-2a, -2b, -2h, -3e, -1c, -1e |

|  |  |
| --- | --- |
| 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** |
| Awareness and Training | **PR.AT-1** | PR.AT-3, PR.AT-4, PR.AT-5 |
| Information Protection Processes & Procedures | **PR.IP-9** | PR.IP-2, PR.IP-5, PR.IP-10, PR.IP-11, PR.IP-12 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| 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 IT and OT roles, responsibilities, and requirements necessary to support MBLT operations.** | * **CCS CSC 9**
* **COBIT 5 APO07.03, BAI05.07**
* **ISA 62443-2-1:2009 4.3.2.4.2**
* **ISO/IEC 27001:2013 A.7.2.2**
* **NIST SP 800-53 Rev. 4 AT-2, PM-13**
 | WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i |
| Awareness and Training | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *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 |
| Awareness and Training | PR.AT-4: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| Awareness and Training | PR.AT-5: Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* | * CCS CSC 9
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, PM-13
 | WM-1a, -1b, -1c, -1d, -1e, -1f, -1g |
| 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-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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed** | **MBLT 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 readiness for audits and inspections.** | * **COBIT 5 DSS04.03**
* **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1**
* **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2**
* **NIST SP 800-53 Rev. 4 CP-2, IR-8**
 | **IR-3f, 3k, -3m, 4c, -4d, -4f, -4i, 4j, -5a, -5b,** **-5c, -5e, -5f, -5g, -5h,** **-5i,** **TVM-1d,** **RM-1c** |
| Information Protection Processes & Procedures | PR.IP-10: Response and recovery plans are tested | *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-3d, 3k, -4f, -4i, -4j |
| 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, -1f, -1g, -1h |
| 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 |

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

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

|  |  |
| --- | --- |
| Respond | When organizations experience a cybersecurity events, the ability to swiftly and effectively respond directly influences their ability to pass future inspections or audits. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Mitigation | **RS.MI-2** | RS.MI-1, RS.MI-3 |
| Improvements | **RS.IM-1** | RS.IM-2 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Mitigation | RS.MI-1: Incidents are contained | *Rationale only provided for High Priority Subcategories* | * 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 pass an audit or inspection.** | * **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** |
| Mitigation | RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | *Rationale only provided for High Priority Subcategories* | * ISO/IEC 27001:2013 A.12.6.1
* NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
 | TVM-2c, -2f, -2g, -2m, -2n, RM-2j |
| Improvements | **RS.IM-1: Recovery plans incorporate lessons learned** | **Lessons learned from responding to a cybersecurity event provide valuable feedback for policy, procedural, and operational improvements that prevent or reduce adverse impacts to MBLT operations and aid the organization in maintaining an acceptable level of readiness for audits and inspections.**  | * **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** |
| Improvements | RS.IM-2: Response strategies are updated |  | * NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
 | IR-3h, -3k |

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

## **A-8 Mission Objective 8: Obtain Timely Vessel Clearance**

|  |
| --- |
| ***Mission Objective 8: Obtain Timely Vessel Clearance***Assure cybersecurity dimension of systems that can impact readiness and operational preparedness. Organizations should:* demonstrate and share documents, data and other items to assure safe and secure entry into a port environment
* ensure confidentiality of sensitive data, plans, and procedures, particularly personnel data and documents
 |

|  |  |
| --- | --- |
| Identify | The business environment and governance practices shape the requirements organizations must meet order to obtain timely vessel clearance. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Business Environment | **ID.BE-4** | ID.BE-3 |
| Governance | **ID.GV-3** | ID.GV-2 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Business Environment | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | *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 MBLT operational activities required for timely vessel clearance. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated MBLT 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** |
| Governance | ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | *Rationale only provided for High Priority Subcategories* | * COBIT 5 APO13.12
* ISA 62443-2-1:2009 4.3.2.3.3
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.1
* NIST SP 800-53 Rev. 4 PM-1, PS-7
 | WM-1a, -1b, -1c, -1e, -1f, -1g, -2d, -5b, ISC-2b  |
| Governance | **ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed** | **Various MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies. Demonstrating adherence to those requirements enables efficient and timely vessel clearance.** | * 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)
 | **CPM-2k,** **IR-3n, -5f,** **RM-3f,** **AACM-4f,** **IAM-3f,** **TVM-3f,** **SA-4f,** **ISC-2f,** **EDM-3f,** **WM-5f** |

|  |  |
| --- | --- |
| Protect | The ability to demonstrate a state of readiness and operational preparedness relies heavily on well documented policies and procedures, and adequate awareness and training activities. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Access Control | N/A | PR.AC-1 |
| Data Security | **PR.DS-6** | PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-5 |
| Information Protection Processes & Procedures | **PR.IP-9** | PR.IP-2, PR.IP-5, 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 | *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 |
| 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 | *Rationale only provided for High Priority Subcategories* | * 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 | *Rationale only provided for High Priority Subcategories* | * 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
 | TVM-1c, -2c, CPM-3b |
| Data Security | **PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity** | **Unauthorized changes to IT or OT software, firmware, or information that support MBLT operations may result in safety, operational, or compliance issues that limit or prevent the organization’s ability to obtain timely vessel clearance. Determining appropriate triggers and frequency for conducting integrity checks and how to respond for assets enables organizations to respond efficiently and effectively when integrity-related cybersecurity events are identified.** | * **ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8**
* **ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3**
* **NIST SP 800-53 Rev. 4 SI-7**
 | **SA-2e, -2i** |
| Information Protection Processes & Procedures | PR.IP-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-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, -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** | **MBLT 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 readiness for obtaining timely vessel clearance.** | * **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 | *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 |

|  |  |
| --- | --- |
| Detect | Detection processes must comply with applicable rules and regulations |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Detection Processes | **DE.DP-2** | DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| 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-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, -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-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 | *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 | When organizations experience a cybersecurity events, their ability to recover directly influences their ability to demonstrate an acceptable state of readiness and operational preparedness for obtaining timely vessel clearance. |
| Categories | **High Priority Subcategories** | **Moderate Priority Subcategories** |
| Communications | N/A | RC.CO-3 |

| Detailed Specifications | Optional Resources |
| --- | --- |
| Category | Subcategory | Rationale for High Priority | Cybersecurity Framework-based Informative References | C2M2 Practices |
| Communications | RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* | * NIST SP 800-53 Rev. 4 CP-2, IR-4
 | IR-3d |

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)