# Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalk

*February 2014*

Homeland Security

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| | | | | | |
| IDENTIFY (ID) | **Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | AM:G2.Q1 (Technology) | ADM:SG1.SP1 | • CCS CSC 1<br>• COBIT 5 BAI03.04, BAI09.01, BAI09.02, BAI09.05<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>• NIST SP 800-53 Rev. 4 CM-8 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | AM:G2.Q1 (Technology) | ADM:SG1.SP1 | • CCS CSC 2<br>• COBIT 5 BAI03.04, BAI09.01, BAI09.02, BAI09.05<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>• NIST SP 800-53 Rev. 4 CM-8 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | AM:G2.Q2 | ADM:SG1.SP2 | • CCS CSC 1<br>• COBIT 5 DSS05.02<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISO/IEC 27001:2013 A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9 |
| | | **ID.AM-4:** External information systems are catalogued | AM:G2.Q1 (Technology) | ADM:SG1.SP1 | • COBIT 5 APO02.02<br>• ISO/IEC 27001:2013 A.11.2.6<br>• NIST SP 500-291 3, 4<br>• NIST SP 800-53 Rev. 4 AC-20, SA-9 |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | AM:G1.Q4 | SC:SG2.SP1 | • COBIT 5 APO03.03, APO03.04, BAI09.02<br>• ISA 62443-2-1:2009 4.2.3.6<br>• ISO/IEC 27001:2013 A.8.2.1<br>• NIST SP 800-34 Rev. 1<br>• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | AM:MIL2.Q3 | ADM:GG2.GP7 | • COBIT 5 APO01.02, DSS06.03<br>• ISA 62443-2-1:2009 4.3.2.3.3<br>• ISO/IEC 27001:2013 A.6.1.1<br>• NIST SP 800-53 Rev. 4 CP-2, PM-11 |
| | **Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | EDM:G2.Q1 | EXD:SG2.SP1 | • COBIT 5 APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02<br>• ISO/IEC 27001:2013 A.15.2<br>• NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| | | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | AM:G1.Q1 | EF:SG1.SP1 | • COBIT 5 APO02.06, APO03.01<br>• NIST SP 800-53 Rev. 4 PM-8 |
| | | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | AM:G1.Q2 | EF:SG1.SP3 | • COBIT 5 APO02.01, APO02.06, APO03.01<br>• ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6<br>• NIST SP 800-53 Rev. 4 PM-11, SA-14 |
| | | **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | EDM:G1.Q1 | EXD:SG1.SP1 | • COBIT 5 DSS01.03<br>• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3<br>• NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |
| | | **ID.BE-5:** Resilience requirements to support delivery of critical services are established | AM:G3.Q2 | RRD:SG2.SP1 | • COBIT 5 DSS04.02<br>• ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>• NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 |
| | **Governance (GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | **ID.GV-1:** Organizational information security policy is established | MIL2.Q2 (All Domains) | GG2.GP1 | • COBIT 5 APO01.03, MEA01.01, EDM01.01, EDM01.02<br>• ISA 62443-2-1:2009 4.3.2.6<br>• ISO/IEC 27001:2013 A.5.1.1<br>• NIST SP 800-53 Rev. 4 -1 controls from all families |
| | | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | MIL2.Q3 (All Domains) | GG2.GP7 | • COBIT 5 APO13.12<br>• ISA 62443-2-1:2009 4.3.2.3.3<br>• ISO/IEC 27001:2013 A.6.1.1<br>• NIST SP 800-53 Rev. 4 AC-21, PM-1, PS-7 |
| | | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | CM:G2.Q1 | CTRL:SG2.SP1<br>COMP:SG2.SP1 | • COBIT 5 MEA03.01, MEA03.04<br>• ISA 62443-2-1:2009 4.4.3.7<br>• ISO/IEC 27001:2013 A.18.1.1, A.18.2.2<br>• NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1), Appendix J |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| | | **ID.GV-4:** Governance and risk management processes address cybersecurity risks | RM:G1.Q3 | RISK:SG1.SP2 | • COBIT 5 DSS04.02<br>• 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<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 PM-9, PM-11 |
| | **Risk Assessment (RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | **ID.RA-1:** Asset vulnerabilities are identified and documented | VM:G2.Q3<br>VM:G2.Q6 | VAR:SG2.SP2 | • CCS CSC 4<br>• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04<br>• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12<br>• ISO/IEC 27001:2013 A.12.6.1, A.18.2.3<br>• NIST SP 800-30 Rev. 1<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, RA-3, RA-5, SI-4, SI-5 |
| | | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | SA:G1.Q1 | MON:SG1.SP2 | • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>• NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 |
| | | **ID.RA-3:** Threats, both internal and external, are identified and documented | SA:G1.Q2 | MON:SG2.SP2 | • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04<br>• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>• NIST SP 800-30 Rev. 1<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-16 |
| | | **ID.RA-4:** Potential business impacts and likelihoods are identified | RM:G4.Q1 | RISK:SG4.SP1 | • COBIT 5 DSS04.02<br>• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>• NIST SP 800-30 Rev. 1<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 |
| | | **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | RM:G3.Q1 | RISK:SG3.SP2 | • COBIT 5 APO12.02<br>• ISO/IEC 27001:2013 A.12.6.1<br>• NIST SP 800-30 Rev. 1<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 |
| | | **ID.RA-6:** Risk responses are identified and prioritized | RM:G5.Q1 | RISK:SG5.SP1 | • COBIT 5 APO12.05, APO13.02<br>• NIST SP 800-53 Rev. 4 PM-4, PM-9 |
| | **Risk Management Strategy (RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | RM:MIL2.Q1 | RISK:GG2.GP2 | • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02<br>• ISA 62443-2-1:2009 4.3.4.2<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 PM-9 |
| | | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | RM:G2.Q4 | RISK:SG2.SP1 | • COBIT 5 APO10.04, APO10.05, APO12.06<br>• ISA 62443-2-1:2009 4.3.2.6.5<br>• NIST SP 800-39<br>• NIST SP 800-53 Rev. 4 PM-9 |
| | | **ID.RM-3:** The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis | RM:G1.Q1<br>RM:G2.Q3 | RISK:SG1.SP1<br>RISK:SG2.SP2 | • NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 |
| | | | | | |
| | **Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | AM:G5.Q1 | AM:SG1.SP1 | • CCS CSC 16<br>• COBIT 5 DSS05.04, DSS06.03<br>• ISA 62443-2-1:2009 4.3.3.5.1<br>• 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<br>• 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<br>• NIST SP 800-53 Rev. 4 AC-2, IA Family |
| | | **PR.AC-2:** Physical access to assets is managed and protected | AM:G5.Q1 | AM:SG1.SP1 | • COBIT 5 DSS01.04, DSS05.05<br>• ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8<br>• ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3<br>• NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 |
| | | **PR.AC-3:** Remote access is managed | AM:G5.Q1 | AM:SG1.SP1 | • COBIT 5 APO13.01, DSS01.04, DSS05.03<br>• ISA 62443-2-1:2009 4.3.3.6.6<br>• ISA 62443-3-3:2013 SR 1.13, SR 2.6<br>• ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC 17, AC-19, AC-20 |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| | | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | AM:G5.Q2 | AM:SG1.SP1 | • CCS CSC 12, 15<br>• ISA 62443-2-1:2009 4.3.3.7.3<br>• ISA 62443-3-3:2013 SR 2.1<br>• ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4<br>• NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 |
| | | **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | CM:G2.Q1 | CTRL:SG2.SP1 | • ISA 62443-2-1:2009 4.3.3.4<br>• ISA 62443-3-3:2013 SR 3.1, SR 3.8<br>• ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1<br>• NIST SP 800-53 Rev. 4 AC-4, SC-7 |
| | **Awareness and Training (AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. | **PR.AT-1:** All users are informed and trained | TA:G2.Q1 | OTA:SG2.SP1 | • CCS CSC 9<br>• COBIT 5 APO07.03, BAI05.07<br>• ISA 62443-2-1:2009 4.3.2.4.2<br>• ISO/IEC 27001:2013 A.7.2.2<br>• NIST SP 800-53 Rev. 4 AT-2, PM-13 |
| | | **PR.AT-2:** Privileged users understand roles & responsibilities. | TA:G2.Q2 | OTA:SG4.SP1 | • CCS CSC 9<br>• COBIT 5 APO07.02<br>• ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3<br>• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2<br>• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| | | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | EDM:G3.Q4 | EXD:SG3.SP4 | • CCS CSC 9<br>• COBIT 5 APO07.03, APO10.04, APO10.05<br>• ISA 62443-2-1:2009 4.3.2.4.2<br>• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2<br>• NIST SP 800-53 Rev. 4 PS-7, SA-9 |
| | | **PR.AT-4:** Senior executives understand roles & responsibilities | TA:G2.Q2 | OTA:SG4.SP1 | • CCS CSC 9<br>• COBIT 5 APO07.03<br>• ISA 62443-2-1:2009 4.3.2.4.2<br>• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,<br>• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| | | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | TA:G2.Q2 | OTA:SG4.SP1 | • CCS CSC 9<br>• COBIT 5 APO07.03<br>• ISA 62443-2-1:2009 4.3.2.4.2<br>• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,<br>• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| | **Data Security (DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | **PR.DS-1:** Data-at-rest is protected | CM:G2.Q1 | CTRL:SG2.SP1<br>KIM:SG4.SP2 | • CCS CSC 17<br>• COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06<br>• ISA 62443-3-3:2013 SR 3.4, SR 4.1<br>• ISO/IEC 27001:2013 A.8.2.3<br>• NIST SP 800-53 Rev. 4 SC-28 |
| | | **PR.DS-2:** Data-in-transit is protected | CM:G2.Q1 | CTRL:SG2.SP1<br>KIM:SG4.SP2 | • CCS CSC 17<br>• COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06<br>• ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2<br>• 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<br>• NIST SP 800-53 Rev. 4 SC-8 |
| | | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | AM:G6.Q7 | KIM:SG4.SP3 | • COBIT 5 BAI09.03<br>• ISA 62443-2-1:2009 4.4.4.4.9<br>• ISA 62443-3-3:2013 SR 4.2<br>• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7<br>• NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 |
| | | **PR.DS-4:** Adequate capacity to ensure availability is maintained | CCM:G1.Q3 | TM:SG5.SP3 | • COBIT 5 APO13.01<br>• ISA 62443-3-3:2013 SR 7.1, SR 7.2<br>• ISO/IEC 27001:2013 A.12.3.1<br>• NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 |
| | | **PR.DS-5:** Protections against data leaks are implemented | CM:G2.Q1 | CTRL:SG2.SP1 | • CCS CSC 17<br>• COBIT 5 APO01.06<br>• ISA 62443-3-3:2013 SR 5.2<br>• ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, 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,<br>• 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 |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| PROTECT (PR) | | **PR.DS-6:** Use of cryptography and cryptographic keys is managed | CM:G2.Q1 | CTRL:SG2.SP1<br>KIM:SG4.SP1 | • COBIT 5 APO01.03, APO10.02, APO10.04, MEA03.01<br>• ISA 62443-3-3:2013 SR 4.1<br>• ISO/IEC 27001:2013 A.14.1.2, A.14.1.3, A.18.1.5<br>• NIST SP 800-53 Rev. 4 SC-12, SC-13 |
| | | **PR.DS-7:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | CCM:G2.Q2<br>CCM:G2.Q5 | TM:SG4.SP3<br>KIM:SG5.SP3 | • COBIT 5 BAI06.01, BAI01.10<br>• ISA 62443-3-3:2013 SR 7.7<br>• ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3<br>• NIST SP 800-53 Rev. 4 SI-7 |
| | | **PR.DS-8:** The development and testing environment(s) are separate from the production environment | CCM:G2.Q7 | TM:SG4.SP4 | • COBIT 5 BAI07.04<br>• ISO/IEC 27001:2013 A.12.1.4<br>• NIST SP 800-53 Rev. 4 CM-2 |
| | **Information Protection Processes and Procedures (IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | CCM:G3.Q1 | TM:SG4.SP2 | • CCS CSC 3, 10<br>• COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05<br>• ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3<br>• ISA 62443-3-3:2013 SR 7.6<br>• 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<br>• NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, SA-10 |
| | | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | CCM:G1.Q1 | ADM:SG3.SP2<br>RTSE:SG2.SP2 | • CCS CSC 6<br>• COBIT 5 APO13.01<br>• ISA 62443-2-1:2009 4.3.4.3.3<br>• ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5<br>• NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, PL-8 |
| | | **PR.IP-3:** Configuration change control processes are in place | CCM:G1.Q1 | ADM:SG3.SP2 | • COBIT 5 BAI06.01, BAI01.06<br>• ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3<br>• ISA 62443-3-3:2013 SR 7.6<br>• 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<br>• NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 |
| | | **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically | AM:G6.Q5 | KIM:SG6.SP1 | • COBIT 5 APO13.01<br>• ISA 62443-2-1:2009 4.3.4.3.9<br>• ISA 62443-3-3:2013 SR 7.3, SR 7.4<br>• ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3<br>• NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 |
| | | **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | AM:G7.Q3 | EC:SG2.SP2 | • COBIT 5 DSS01.04, DSS05.05<br>• 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<br>• ISO/IEC 27001:2013 A.11.1.4, A.11.2.2<br>• NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| | | **PR.IP-6:** Data is destroyed according to policy | AM:G6.Q7 | KIM:SG4.SP3 | • COBIT 5 BAI09.03<br>• ISA 62443-2-1:2009 4.3.4.4.4<br>• ISA 62443-3-3:2013 SR 4.2<br>• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7<br>• NIST SP 800-53 Rev. 4 MP-6 |
| | | **PR.IP-7:** Protection processes are continuously improved | MIL4.Q1<br>(All Domains) | GG2.GP8 | • COBIT 5 APO11.06, DSS04.05<br>• 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<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 |
| | | **PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties | SA:G2.Q1<br>SA:G2.Q2 | COMM:SG1.SP1 | • COBIT 5 DSS04.03<br>• ISO/IEC 27001:2013 A.16.1.6<br>• NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 |
| | | **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | SCM:G1.Q1<br>IM:G1.Q1 | SC:SG3.SP2<br>IMC:SG1.SP1 | • COBIT 5 DSS04.03<br>• ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1<br>• ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2<br>• NIST SP 800-53 Rev. 4 CP-2, IR-8 |
| | | **PR.IP-10:** Response and recovery plans are tested | SCM:G3.Q3<br>IM:G1.Q2 | SC:SG5.SP3<br>IMC:SG1.SP1 | • ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11<br>• ISA 62443-3-3:2013 SR 3.3<br>• ISO/IEC 27001:2013 A.17.1.3<br>• NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 |
| | | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | CM:G2.Q1 | CTRL:SG2.SP1<br>HRM:SG3.SP1 | • COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05<br>• ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3<br>• ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4<br>• NIST SP 800-53 Rev. 4 PS Family |
| | | **PR.IP-12:** A vulnerability management plan is developed and implemented | VM:G1Q1 | VAR:SG1.SP2 | • ISO/IEC 27001:2013 A.12.6.1, A.18.2.2<br>• NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| | **Maintenance (MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | CCM:G1.Q1 | ADM:SG3.SP2 | • COBIT 5 BAI09.03<br>• ISA 62443-2-1:2009 4.3.3.3.7<br>• ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5<br>• NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 |
| | | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | CCM:G1.Q1 | ADM:SG3.SP2 | • COBIT 5 DSS05.04<br>• 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<br>• ISO/IEC 27001:2013 A.11.2.4<br>• NIST SP 800-53 Rev. 4 MA-4 |
| | **Protective Technology (PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-1**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | CM:G2.Q1 | CTRL:SG2.SP1<br>MON:SG1.SP3 | • CCS CSC 14<br>• COBIT 5 APO11.04<br>• 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<br>• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12<br>• ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1<br>• NIST SP 800-53 Rev. 4 AU Family |
| | | **PR.PT-2:** Removable media is protected and its use restricted according to policy | CM:G2.Q1 | CTRL:SG2.SP1<br>TM:SG2.SP2 | • COBIT 5 DSS05.02, APO13.01<br>• ISA 62443-3-3:2013 SR 2.3<br>• ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9<br>• NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7, SC-44 |
| | | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | AM:G5.Q1 | AM:SG1.SP1 | • CCS CSC 6<br>• COBIT 5 DSS05.02<br>• 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<br>• 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<br>• ISO/IEC 27001:2013 A.9.1.2<br>• NIST SP 800-53 Rev. 4 AC-3, CM-7 |
| | | **PR.PT-4:** Communications and control networks are protected | CM:G2.Q1 | CTRL:SG2.SP1<br>TM:SG2.SP2 | • CCS CSC 7<br>• COBIT 5 DSS05.02, APO13.01<br>• 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<br>• ISO/IEC 27001:2013 A.13.1.1, A.13.2.1,<br>• NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 |
| | | | | | |
| | **Anomalies and Events (AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | CCM:G3.Q1 | TM:SG4.SP2 | • COBIT 5 DSS03.01<br>• ISA 62443-2-1:2009 4.4.3.3<br>• NIST SP 800-53 Rev. 4 AC-4, CM-2, SI-4 |
| | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | IM:G2.Q4 | IMC:SG2.SP4 | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>• 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<br>• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 |
| | | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | IM:G2.Q4 | IMC:SG2.SP4 | • ISA 62443-3-3:2013 SR 6.1<br>• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, SI-4 |
| | | **DE.AE-4:** Impact of events is determined | IM:G2.Q5 | IMC:SG2.SP4 | • COBIT 5 APO12.06<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 |
| | | **DE.AE-5:** Incident alert thresholds are established | IM:G3.Q2 | IMC:SG3.SP1 | • COBIT 5 APO12.06<br>• ISA 62443-2-1:2009 4.2.3.10<br>• NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8<br>• NIST SP 800-61 Rev 2 |
| | **Security Continuous Monitoring (CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | IM:G2.Q1 | IMC:SG2.SP1 | • CCS CSC 14, 16<br>• COBIT 5 DSS05.07<br>• ISA 62443-3-3:2013 SR 6.2<br>• NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 |
| | | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | IM:G2.Q1 | IMC:SG2.SP1 | • ISA 62443-2-1:2009 4.3.3.3.8<br>• NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 |
| | | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | IM:G2.Q1 | IMC:SG2.SP1 | • ISA 62443-3-3:2013 SR 6.2<br>• ISO/IEC 27001:2013 A.12.4.1<br>• NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| DETECT (DE) | | **DE.CM-4:** Malicious code is detected | VM:G1.Q2 | VAR:SG1.SP2 | • CCS CSC 5<br>• COBIT 5 DSS05.01<br>• ISA 62443-2-1:2009 4.3.4.3.8<br>• ISA 62443-3-3:2013 SR 3.2<br>• ISO/IEC 27001:2013 A.12.2.1<br>• NIST SP 800-53 Rev. 4 SI-3 |
| | | **DE.CM-5:** Unauthorized mobile code is detected | VM:G1.Q2 | VAR:SG1.SP2 | • ISA 62443-3-3:2013 SR 2.4<br>• ISO/IEC 27001:2013 A.12.5.1<br>• NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 |
| | | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | EDM:G4.Q1 | EXD:SG4.SP1 | • COBIT 5 APO07.06<br>• ISO/IEC 27001:2013 A.14.2.7, A.15.2.1<br>• NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 |
| | | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | VM:G1.Q2 | VAR:SG1.SP2 | • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |
| | | **DE.CM-8:** Vulnerability scans are performed | VM:G2.Q3 | VAR:SG2.SP2 | • COBIT 5 BAI03.10<br>• ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7<br>• ISO/IEC 27001:2013 A.12.6.1<br>• NIST SP 800-53 Rev. 4 RA-5 |
| | **Detection Processes (DP):** Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | IM:G1.Q1 | IMC:SG1.SP1 | • CCS CSC 5<br>• COBIT 5 DSS05.01<br>• ISA 62443-2-1:2009 4.4.3.1<br>• ISO/IEC 27001:2013 A.6.1.1<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 |
| | | **DE.DP-2:** Detection activities comply with all applicable requirements | IM:G2.Q8 | IMC:SG2.SP3<br>MON:SG1.SP4 | • ISA 62443-2-1:2009 4.4.3.2<br>• ISO/IEC 27001:2013 A.18.1.4<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 |
| | | **DE.DP-3:** Detection processes are tested | IM:MIL4.Q1 | IMC:GG2.GP8 | • COBIT 5 APO13.02<br>• ISA 62443-2-1:2009 4.4.3.2<br>• ISA 62443-3-3:2013 SR 3.3<br>• ISO/IEC 27001:2013 A.14.2.8<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 |
| | | **DE.DP-4:** Event detection information is communicated to appropriate parties | IM:G2.Q1 | IMC:SG2.SP1 | • COBIT 5 APO12.06<br>• ISA 62443-2-1:2009 4.3.4.5.9<br>• ISA 62443-3-3:2013 SR 6.1<br>• NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, PL-2, RA-5, SI-4 |
| | | **DE.DP-5:** Detection processes are continuously improved | IM:G5.Q3 | IMC:SG5.SP3 | • COBIT 5 APO11.06, DSS04.05<br>• ISA 62443-2-1:2009 4.4.3.4<br>• ISO/IEC 27001:2013 A.16.1.6<br>• NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |
| | | | | | |
| | **Response Planning (RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. | **RS.RP-1:** Response plan is executed during or after an event | IM:G4.Q2 | IMC:SG4.SP2 | • COBIT 5 BAI01.10<br>• CCS CSC 18<br>• ISA 62443-2-1:2009 4.3.4.5.1<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 |
| | **Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | IM:G1.Q4 | IMC:SG1.SP2 | • COBIT 5 BAI04.02<br>• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4<br>• ISO/IEC 27001:2013 A.6.1.1<br>• NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 |
| | | **RS.CO-2:** Events are reported consistent with established criteria | IM:G2.Q1 | IMC:SG2.SP1 | • COBIT 5 BAI01.10<br>• ISA 62443-2-1:2009 4.3.4.5.5<br>• ISO/IEC 27001:2013 A.16.1.2<br>• NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 |
| | | **RS.CO-3:** Information is shared consistent with response plans | IM:G4.Q3 | IMC:SG4.SP3 | • COBIT 5 DSS01.03<br>• ISA 62443-2-1:2009 4.3.4.5.2<br>• ISO/IEC 27001:2013 A.16.1.2<br>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | IM:G4.Q1 | IMC:SG4.SP1 | • COBIT 5 DSS02.01<br>• ISA 62443-2-1:2009 4.3.4.5.5<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |

| Function | Category | Subcategory | CRR Reference | RMM Reference | Informative References |
|---|---|---|---|---|---|
| RESPOND (RS) | | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | SA:G2.Q2 | COMM:SG1.SP1 | • COBIT 5 APO12.01<br>• NIST SP 800-53 Rev. 4 PM-15, SI-5 |
| | **Analysis (AN):** Analysis is conducted to ensure adequate response and support recovery activities. | **RS.AN-1:** Notifications from detection systems are investigated | IM:G2.Q7 | IMC:SG2.SP4 | • COBIT 5 DSS02.07<br>• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>• ISA 62443-3-3:2013 SR 6.1<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 |
| | | **RS.AN-2:** The impact of the incident is understood | IM:G3.Q3 | IMC:SG3.SP2 | • COBIT 5 BAI01.11<br>• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4 |
| | | **RS.AN-3:** Forensics are performed | IM:G2.Q9 | IMC:SG2.SP3 | • 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<br>• ISO/IEC 27001:2013 A.16.1.7<br>• NIST SP 800-53 Rev. 4 AU-7, IR-4 |
| | | **RS.AN-4:** Incidents are categorized consistent with response plans | IM:G3.Q3 | IMC:SG3.SP2 | • ISA 62443-2-1:2009 4.3.4.5.6<br>• ISO/IEC 27001:2013 A.16.1.4<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 |
| | **Mitigation (MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | **RS.MI-1:** Incidents are contained | IM:G4.Q2 | IMC:SG4.SP2 | • ISA 62443-2-1:2009 4.3.4.5.6<br>• ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 IR-4 |
| | | **RS.MI-2:** Incidents are mitigated | IM:G4.Q4 | IMC:SG4.SP4 | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 IR-4 |
| | | **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | VM:G3.Q1 | VAR:SG2.SP3 | • ISO/IEC 27001:2013 A.12.6.1<br>• NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 |
| | **Improvements (IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **RS.IM-1:** Response plans incorporate lessons learned | IM:G5.Q3 | IMC:SG5.SP3 | • COBIT 5 BAI01.13<br>• ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4<br>• ISO/IEC 27001:2013 A.16.1.6<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
| | | **RS.IM-2:** Response strategies are updated | IM:G5.Q3 | IMC:SG5.SP3 | • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
| | | | | | |
| RECOVER (RC) | **Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. | **RC.RP-1:** Recovery plan is executed during or after an event | SCM:G4.Q1 | SC:SG6.SP1 | • CCS CSC 8<br>• COBIT 5 DSS02.05, DSS03.04<br>• ISO/IEC 27001:2013 A.16.1.5<br>• NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 |
| | **Improvements (IM):** Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | SCM:G4.Q3 | SC:SG7.SP2 | • COBIT 5 BAI05.07<br>• ISA 62443-2-1 4.4.3.4<br>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
| | | **RC.IM-2:** Recovery strategies are updated | SCM:G4.Q3 | SC:SG7.SP2 | • COBIT APO05.04, BAI07.08<br>• NIST SP 800-53 Rev. 4 CP-2 |
| | **Communications (CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | **RC.CO-1:** Public Relations are managed | IM:G4.Q3 | IMC:SG4.SP3 | • COBIT 5 EDM03.02 |
| | | **RC.CO-2:** Reputation after an event is repaired | RM:G2:Q1<br>RM:G2.Q4 | RISK:SG2.SP2<br>RISK:SG2.SP1 | • COBIT 5 MEA03.02 |
| | | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | IM:G4.Q1 | IMC:SG4.SP1 | • NIST SP 800-53 Rev. 4 CP-2, IR-4 |

| Cyber Resilience Review (CRR) Reference Key | |
|---|---|
| **AM** | Asset Management |
| **CCM** | Configuration and Change Management |
| **CM** | Controls Management |
| **EDM** | External Dependencies Management |
| **IM** | Incident Management |
| **RM** | Risk Management |
| **SA** | Situational Awareness |
| **SCM** | Service Continuity Management |
| **TA** | Training and Awareness |
| **VM** | Vulnerability Management |
| **G*x*** | Goal |
| **Q*x*** | Question |

| Reference | |
|---|---|
| **RMM** | http://www.cert.org/resilience/rmm.html |

| CERT® Resilience Management Model (CERT®-RMM) Reference Key | |
|---|---|
| **ADM** | Asset Definition and Management |
| **AM** | Access Management |
| **COMM** | Communications |
| **COMP** | Compliance |
| **CTRL** | Controls Management |
| **EC** | Environmental Control |
| **EF** | Enterprise Focus |
| **EXD** | External Dependencies Management |
| **HRM** | Human Resource Management |
| **IMC** | Incident Management and Control |
| **KIM** | Knowledge and Information Management |
| **MON** | Monitoring |
| **OTA** | Organizational Training and Awareness |
| **RISK** | Risk Management |
| **RRD** | Resilience Requirements Development |
| **RTSE** | Resilience Technical Solution Engineering |
| **SC** | Service Continuity |
| **TM** | Technology Management |
| **VAR** | Vulnerability Awareness and Resolution |
| **SG*x*** | Specific Goal |
| **SP*x*** | Specific Practice |
| **GG*x*** | Generic Goal |
| **GP*x*** | Generic Practice |


Homeland
Security