Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks

February 2016

Homeland Security

Contents

NIST Cybersecurity Framework (CSF) to Cyber Resilience Review (CRR) Crosswalk

NIST Cybersecurity Framework (CSF) to Cyber Resilience Review (CRR) Crosswalk

Function	Category	Subcategory	CRR References *	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. **CRR References** AM:G2.Q1 – PIF AM:G2.Q3 – PITF AM:G2.Q4 – PITF AM:G4.Q1 – PITF AM:G4.Q2 - PITF AM:MIL2.Q1 AM:MIL2.Q4	**ID.AM-1:** Physical devices and systems within the organization are inventoried	AM:G2.Q1 - T	• 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
		ID.AM-2: Software platforms and applications within the organization are inventoried	AM:G2.Q1 - T	• 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
		ID.AM-3: Organizational communication and data flows are mapped	AM:G2.Q5	• 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
		ID.AM-4: External information systems are catalogued	AM:G2.Q1 - T	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • 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.Q2 AM:G7.Q1 AM:G7.Q2	• 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
		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, IM:MIL2.Q3, EDM:MIL2.Q3 CM:MIL2.Q3, SCM:MIL2.Q3, TA:MIL2.Q3 CCM:MIL2.Q3, RM:MIL2.Q3, SA:MIL2.Q3 VM:MIL2.Q3, EDM:G4.Q2	• 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
	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. **CRR References** AM:G1.Q1, SCM:MIL3.Q3 AM:G1.Q2, RM:MIL3.Q3 AM:MIL3.Q3, EDM:MIL2.Q1 CM:MIL3.Q3, EDM:MIL2.Q4 CCM:MIL3.Q3, EDM:MIL3.Q3 VM:MIL3.Q3, TA:MIL3.Q3 IM:MIL3.Q3, SA:MIL3.Q3	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	EDM:G2.Q1, EDM:G3.Q3, EDM:G4.Q2 EDM:G3.Q1, EDM:G3.Q4, EDM:G4.Q3 EDM:G3.Q2, EDM:G4.Q1, EDM:G4.Q4	• COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	AM:G1.Q3	• COBIT 5 APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	AM:G1.Q4	• 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
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	AM:G3.Q1 – PITF, EDM:G1.Q1, EDM:G3.Q3 AM:G7.Q1, EDM:G1.Q2, EDM:G5.Q1 AM:G7.Q2, EDM:G1.Q3, EDM:G5.Q2	• 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
		ID.BE-5: Resilience requirements to support delivery of critical services are established	AM:G2.Q2 - PITF, SCM:G1.Q6, EDM:G3.Q3 AM:G3.Q2 – PITF, EDM:G3.Q1, EDM:G3.Q4 AM:G7.Q3, EDM:G3.Q2	• 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

* RMM references for the CRR questions can be found in the CRR to CSF Crosswalk starting on page 13.

Function	Category	Subcategory	CRR References	Informative References
Identify (ID)	**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	AM:MIL2.Q2 CM:MIL2.Q2 CCM:MIL2.Q2 VM:MIL2.Q2 IM:MIL2.Q2 SCM:MIL2.Q2 RM:MIL2.Q2 EDM:MIL2.Q2 TA:MIL2.Q2 SA:MIL2.Q2	• 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
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	AM:MIL2.Q3 CM:MIL2.Q3 CCM:MIL2.Q3 VM:MIL2.Q3 IM:MIL2.Q3 SCM:MIL2.Q3 RM:MIL2.Q3 EDM:MIL2.Q3 TA:MIL2.Q3 SA:MIL2.Q3	• 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
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	AM:G3.Q2 – PITF CM:G1.Q1 – PITF CM:G1.Q2 CM:G2.Q1 IM:G2.Q8 IM:G2.Q9	• 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)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	AM:MIL3.Q4 CM:MIL3.Q4 CCM:MIL3.Q4 VM:MIL3.Q4 IM:MIL3.Q4 SCM:MIL3.Q4 RM:G1.Q3 RM:MIL3.Q4 EDM:MIL3.Q4 TA:MIL3.Q4 SA:MIL3.Q4	• 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
	Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. **CRR References** SA:MIL2.Q1 SA:MIL2.Q4	**ID.RA-1:** Asset vulnerabilities are identified and documented	VM:G2.Q3 – ITF VM:G2.Q6 - ITF	• 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
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	VM:G2.Q1 – ITF VM:G2.Q2 – ITF SA:G1.Q1	• 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
		ID.RA-3: Threats, both internal and external, are identified and documented	SA:G1.Q2	• 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
		ID.RA-4: Potential business impacts and likelihoods are identified	RM:G2.Q1 RM:G2.Q2 RM:G4.Q1	• 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
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RM:G3.Q1 EDM:G2.Q1	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	AM:MIL3.Q4 CM:MIL3.Q4 CCM:MIL3.Q4 VM:MIL3.Q4 IM:MIL3.Q4 SCM:MIL3.Q4 RM:G4.Q2 RM:G5.Q1 RM:G5.Q2 RM:MIL3.Q4 EDM:MIL3.Q4 TA:MIL3.Q4 SA:MIL3.Q4	• COBIT 5 APO12.05, APO13.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9

Function	Category	Subcategory	CRR References	Informative References
Identify (ID)	**Risk Management Strategy (RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. **CRR References** RM:G1.Q1 RM:G1.Q2 RM:G2.Q2 RM:G5.Q1 RM:G5.Q2	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	RM:G1.Q3 RM:G1.Q4 RM:MIL2.Q1 RM:MIL2.Q4	• 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
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	RM:G2.Q3 RM:G2.Q4	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • 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:G2.Q3 RM:G2.Q4	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
Protect (PR)	**Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **CRR References** AM:G5.Q3 – ITF AM:G5.Q4 – ITF CM:G1.Q1 – PITF CM:G1.Q2 CM:G2.Q1 CM:MIL2.Q1 CM:MIL2.Q4 CCM:G2.Q8 CCM:MIL2.Q1 CCM:MIL2.Q4	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	AM:G5.Q1 - ITF AM:G5.Q2 - ITF	• 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
		PR.AC-2: Physical access to assets is managed and protected	AM:G5.Q1 – ITF AM:G5.Q2 – ITF	• 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, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	AM:G5.Q1 – ITF AM:G5.Q2 – ITF	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AM:G5.Q5 – ITF AM:G5.Q6 – ITF CCM:G2.Q4	• 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
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	CM:G2.Q2	• 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
	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. **CRR References** AM:MIL2.Q3 RM:MIL2.Q3 AM:MIL3.Q2 RM:MIL3.Q2 CM:MIL2.Q3 EDM:MIL2.Q3 CM:MIL3.Q2 EDM:MIL3.Q2 CCM:MIL2.Q3 TA:G2.Q3	**PR.AT-1:** All users are informed and trained	AM:G6.Q4 TA:G1.Q3 TA:G2.Q2 TA:G1.Q1 TA:G1.Q4 SA:G3.Q3 TA:G1.Q2 TA:G2.Q1	• 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
		PR.AT-2: Privileged users understand roles & responsibilities.	TA:G2.Q5	• 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

Function	Category	Subcategory	CRR References	Informative References
Protect (PR)	**CRR References, cont.** CCM:MIL3.Q2 TA:G2.Q4 VM:MIL2.Q3 TA:MIL2.Q1 VM:MIL3.Q2 TA:MIL2.Q3 IM:MIL2.Q3 TA:MIL2.Q4 IM:MIL3.Q2 TA:MIL3.Q2 SCM:MIL2.Q3 SA:MIL2.Q3 SCM:MIL3.Q2 SA:MIL3.Q2	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	EDM:G3.Q4	• 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
		PR.AT-4: Senior executives understand roles & responsibilities	TA:G2.Q6	• 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
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	TA:G2.Q7 SA:G3.Q2 SA:G1.Q1 SA:G3.Q3 SA:G1.Q3	• 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
	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. **CRR References** AM:G6.Q1 AM:G6.Q2 AM:G6.Q3 CM:G1.Q1 – PITF CM:G1.Q2 CM:G2.Q1 CM:MIL2.Q1 CM:MIL2.Q4 CCM:MIL2.Q1 CCM:MIL2.Q4	**PR.DS-1:** Data-at-rest is protected	CM:G2.Q3	• 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
		PR.DS-2: Data-in-transit is protected	CM:G2.Q4	• 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
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	AM:G6.Q6 AM:G6.Q7	• 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
		PR.DS-4: Adequate capacity to ensure availability is maintained	CCM:G1.Q3	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.3.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	CM:G2.Q5	• 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
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	CCM:G2.Q2 CCM:G2.Q5	• 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
		PR.DS-7: The development and testing environment(s) are separate from the production environment	CCM:G2.Q7	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2

Function	Category	Subcategory	CRR References	Informative References
Protect (PR)	**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. **CRR References** AM:MIL2.Q2 AM:MIL5.Q1 AM:MIL5.Q2 CM:G1.Q1 – PITF CM:G1.Q2 CM:G2.Q1 CM:MIL2.Q1 CM:MIL2.Q2 CM:MIL2.Q4 CM:MIL5.Q1 CM:MIL5.Q2 CCM:MIL2.Q1 CCM:MIL2.Q2 CCM:MIL2.Q4 CCM:MIL5.Q1 CCM:MIL5.Q2 VM:MIL2.Q2 VM:MIL5.Q1 VM:MIL5.Q2 IM:MIL2.Q2 IM:MIL5.Q1 IM:MIL5.Q2 SCM:MIL2.Q2 SCM:MIL5.Q1 SCM:MIL5.Q2 RM:MIL2.Q2 RM:MIL5.Q1 RM.MIL5.Q2 EDM:MIL2.Q2 EDM:MIL5.Q1 EDM:MIL5.Q2 TA:MIL2.Q2 TA:MIL5.Q1 TA:MIL5.Q2 SA:MIL2.Q2 SA:MIL5.Q1 SA:MIL5.Q2	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	CCM:G2.Q1 CCM:G2.Q3 CCM:G3.Q1 CCM:G3.Q2	• 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
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	CCM:G1.Q6	• 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, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	CCM:G1.Q1 – ITF CCM:G1.Q2 – ITF CCM:G1.Q4 CCM:G1.Q5 CCM:G2.Q3 CCM:G2.Q4 CCM:G2.Q6 CCM:G3.Q2	• COBIT 5 BAI06.01, BAI01.06 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	AM:G6.Q5 SCM:G3.Q4	• 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
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	AM:G7.Q3	• 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
		PR.IP-6: Data is destroyed according to policy	AM:G6.Q6 AM:G6.Q7	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.4.4.4 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Protection processes are continuously improved	AM:MIL4.Q1 AM:MIL4.Q2 CM:G3.Q1 – PITF CM:G3.Q2 CM:G4.Q1 – PITF CM:G4.Q2 CM:MIL4.Q1 CM:MIL4.Q2 CCM:MIL4.Q1 CCM:MIL4.Q2 VM:G2.Q2 – ITF VM:G3.Q2 VM:MIL4.Q1 VM:MIL4.Q2 IM:G5.Q1 IM:G5.Q2 IM:G5.Q3 IM:MIL4.Q1 IM:MIL4.Q2 SCM:MIL4.Q1 SCM:MIL4.Q2 RM:MIL4.Q1 RM:MIL4.Q2 EDM:MIL4.Q1 EDM:MIL4.Q2 TA:G2.Q3 TA:G2.Q4 TA:MIL4.Q1 TA:MIL4.Q2 SA:MIL4.Q1 SA:MIL4.Q2	• 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

Function	Category	Subcategory	CRR References	Informative References
Protect (PR)		**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	AM:MIL3.Q1, AM:MIL4.Q3, CM:MIL3.Q1, CM:MIL4.Q3, CCM:MIL3.Q1, CCM:MIL4.Q3, VM:MIL3.Q1, VM:MIL4.Q3, IM:MIL3.Q1, IM:MIL4.Q3, SCM:MIL3.Q1, SCM:MIL4.Q3, RM:MIL3.Q1, RM:MIL4.Q3, EDM:MIL3.Q1, EDM:MIL4.Q3, TA:MIL3.Q1, TA:MIL4.Q3, SA:G2.Q1, SA:G2.Q2, SA:G3.Q1, SA:MIL3.Q1, SA:MIL4.Q3	• ISO/IEC 27001:2013 A.16.1.6 • 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	IM:G1.Q1, IM:MIL2.Q1, IM:MIL2.Q4, SCM:G1.Q1 – PITF, SCM:G1.Q2, SCM:G1.Q3, SCM:G1.Q4, SCM:G1.Q5, SCM:G1.Q6, SCM:G2.Q1, SCM:G4.Q1, SCM:G4.Q2, SCM:MIL2.Q1, SCM:MIL2.Q4	• 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
		PR.IP-10: Response and recovery plans are tested	IM:G1.Q2, SCM:G3.Q1, SCM:G3.Q2, SCM:G3.Q3, SCM:G3.Q5	• 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
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	CM:G2.Q9, CCM:G2.Q4, IM:G1.Q3	• 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
		PR.IP-12: A vulnerability management plan is developed and implemented	VM:G1.Q1 – PITF, VM:G2.Q4 – ITF, VM:G2.Q5 – ITF, VM:G2.Q6 – ITF, VM:G3.Q3, VM:G4.Q1, VM:MIL2.Q1, VM:MIL2.Q4	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **CRR References** CM:G1.Q1 – PITF, CM:G1.Q2, CM:G2.Q1, CM:MIL2.Q1, CM:MIL2.Q4, CCM:MIL2.Q1, CCM:MIL2.Q4	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	CCM:G2.Q9, CCM:G2.Q10	• 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
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	CCM:G2.Q11	• 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
	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. **CRR References** CM:G1.Q1 – PITF, CM:G1.Q2, CM:G2.Q1, CM:MIL2.Q1, CM:MIL2.Q4	**PR.PT-1**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CM:G2.Q6	• 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
		PR.PT-2: Removable media is protected and its use restricted according to policy	CM:G2.Q7	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7

Function	Category	Subcategory	CRR References	Informative References
Protect (PR)		**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality	CM:G2.Q10	• 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
		PR.PT-4: Communications and control networks are protected	CM:G2.Q8	• 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
Detect (DE)	**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.Q3 CCM:G3.Q5 CCM:G3.Q6 CCM:G3.Q4	• 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
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	IM:G2.Q4	• 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, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	IM:G2.Q2 IM:G2.Q6 IM:G2.Q7 IM:G2.Q4	• ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	IM:G2.Q5	• COBIT 5 APO12.06 • 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	• 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
	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. **CRR Reference** VM:G1.Q2 - PITF	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	IM:G2.Q1	• 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
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	IM:G2.Q1	• ISA 62443-2-1:2009 4.3.3.3.8 • 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	• 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
		DE.CM-4: Malicious code is detected	VM:G1.Q3	• 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

Function	Category	Subcategory	CRR References	Informative References
Detect (DE)		**DE.CM-5:** Unauthorized mobile code is detected	VM:G1.Q4	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	EDM:G4.Q1	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	VM:G1.Q5	• 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 - ITF	• 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
	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 IM:G1.Q3 IM:G1.Q4	• 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
		DE.DP-2: Detection activities comply with all applicable requirements	IM:G2.Q8	• 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
		DE.DP-3: Detection processes are tested	IM:MIL4.Q1	• 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
		DE.DP-4: Event detection information is communicated to appropriate parties	IM:G2.Q1	• 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
		DE.DP-5: Detection processes are continuously improved	VM:G2.Q2 – ITF IM:G1.Q2 IM:G5.Q2 VM:G3.Q2 IM:G5.Q1 IM:G5.Q3	• 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
Respond (RS)	**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	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	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 SCM:G1.Q3	• 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
		RS.CO-2: Events are reported consistent with established criteria	IM:G2.Q1 IM:G3.Q1	• 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
		RS.CO-3: Information is shared consistent with response plans	IM:G4.Q3	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

Function	Category	Subcategory	CRR References	Informative References
Respond (RS)		**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	IM:G4.Q1 SCM:G1.Q4	• ISA 62443-2-1:2009 4.3.4.5.5 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SA:G2.Q2 SA:G3.Q1	• 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	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	IM:G3.Q3	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Forensics are performed	IM:G2.Q9	• 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 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	IM:G2.Q3 IM:G3.Q3	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • 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 IM:G4.Q4	• 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
		RS.MI-2: Incidents are mitigated	IM:G4.Q4	• 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
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	VM:G3.Q1	• ISO/IEC 27001:2013 A.12.6.1 • 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. **CRR References** VM:G3.Q2 VM:G4.Q1	**RS.IM-1:** Response plans incorporate lessons learned	IM:G5.Q3	• 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
		RS.IM-2: Response strategies are updated	IM:G5.Q3	• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Function	Category	Subcategory	CRR References	Informative References
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	• 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
	Improvements (IM): Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. **CRR References** SCM:G2.Q1 SCM:G3.Q5 SCM:G4.Q2	**RC.IM-1:** Recovery plans incorporate lessons learned	SCM:G4.Q3	• COBIT 5 BAI05.07 • ISA 62443-2-1 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	SCM:G4.Q3	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	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	• COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	RM:G2.Q1 RM:G2.Q4	• COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	IM:G4.Q1 IM:G4.Q3 SCM:G1.Q4	• 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
Gx	Goal
Qx	Question

References	
CRR	http://www.us-cert.gov/ccubedvp/self-service-crr
RMM	http://www.cert.org/resilience/products-services/cert-rmm/index.cfm

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
SGx	Specific Goal
SPx	Specific Practice
GGx	Generic Goal
GPx	Generic Practice

* RMM references for the CRR questions can be found in the CRR to CSF Crosswalk starting on page 13.

Cyber Resilience Review (CRR) to NIST Cybersecurity Framework (CSF) Crosswalk

Cyber Resilience Review (CRR) to NIST Cybersecurity Framework (CSF) Crosswalk

	CRR Self-Assessment		NIST CSF References	Notes
	1 Asset Management The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.			
	Goal 1—Services are identified and prioritized			
	1.	Are services identified? [SC:SG2.SP1] **	**ID.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.	The concept of a service is not directly addressed. Services support the organizational mission and therefore, the question is mapped to the NIST-CSF category of ID.BE.
	2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value **ID.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.	
	3.	Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified and communicated? [EF:SG1.SP1]	**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated	
	4.	Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated	
	Goal 2—Assets are inventoried, and authority and responsibility for these assets is established.			
	1.	Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1]		
		People	**ID.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.	
		Information	**ID.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.	
		Technology	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ID.AM-2**: Software platforms and applications within the organization are inventoried **ID.AM-4**: External information systems are catalogued	
		Facilities	**ID.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.	
	2.	Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established	
		People		
		Information		
		Technology		
		Facilities		

** Denotes RMM reference with format of [Process Area: Specific Goal.Specific Practice].

	CRR Self-Assessment		NIST CSF References	Notes
	3.	Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	**ID.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.	
		People		
		Information		
		Technology		
		Facilities		
	4.	Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	**ID.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.	
		People		
		Information		
		Technology		
		Facilities		
	5.	Are organizational communications and data flows mapped and documented in the asset inventory? [ADM:SG1.SP2]	**ID.AM-3:** Organizational communication and data flows are mapped	
	Goal 3—The relationship between assets and the services they support is established.			
	1.	Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
		People		
		Information		
		Technology		
		Facilities		
	2.	Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
		People		
		Information		
		Technology		
		Facilities		
	Goal 4—The asset inventory is managed.			
	1.	Have change criteria been established for asset descriptions? [ADM:SG3.SP1]	**ID.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.	This is criteria for the asset description and part of the asset management process not general change management.
		People		
		Information		
		Technology		
		Facilities		
	2.	Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]	**ID.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.	This is criteria for the asset description and part of the asset management process not general change management.
		People		
		Information		
		Technology		
		Facilities		
	Goal 5—Access to assets is managed.			
	1.	Is access (including identities and credentials) to assets granted based on their protection requirements? [AM:SG1.SP1]	**PR.AC-1:** Identities and credentials are managed for authorized devices and users **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed	
		Information		
		Technology		
		Facilities		

	CRR Self-Assessment		NIST CSF References	Notes
	2.	Are access (including identities and credentials) requests reviewed and approved by the asset owner? [AM:SG1.SP1] *Information* *Technology* *Facilities*	**PR.AC-1:** Identities and credentials are managed for authorized devices and users **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed	
	3.	Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3] *Information* *Technology* *Facilities*	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	The review of access privileges applies to the entire category.
	4.	Are access privileges modified as a result of reviews? [AM:SG1.SP4] *Information* *Technology* *Facilities*	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	The review of access privileges applies to the entire category.
	5.	Are access permissions managed Incorporating the principle of least privilege? [AM.SG1.SP1] *Information* *Technology* *Facilities*	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties	
	6.	Are access permissions managed incorporating the principle of separation of duties? [AM.SG1.SP1] *Information* *Technology* *Facilities*	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties	
	Goal 6—Information assets are categorized and managed to ensure the sustainment and protection of the critical service.			
	1.	Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)? [KIM:SG1.SP2]	**PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	2.	Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]	**PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	3.	Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]	**PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	4.	Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories? [KIM:SG1.SP2]	**PR.AT-1:** All users are informed and trained	
	5.	Are high-value information assets backed-up and retained? [KIM:SG6.SP1]	**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically	
	6.	Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	**PR.DS-3**: Assets are formally managed throughout removal, transfers, and disposition **PR.IP-6:** Data is destroyed according to policy	
	7.	Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition **PR.IP-6:** Data is destroyed according to policy	

		CRR Self-Assessment	NIST CSF References	Notes
	Goal 7—Facility assets supporting the critical service are prioritized and managed.			
	1.	Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities? [EC:SG1.SP1]	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	Facilities are referenced in the overall NIST-CSF category description for ID.AM.
	2.	Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
	3.	Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met	
MIL2-Planned	1.	Is there a documented plan for performing asset management activities?	**ID.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.	The ID.AM category is mapped to this question as all of the subcategories should be addressed by the plan.
	2.	Is there a documented policy for asset management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for asset management activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have asset management standards and guidelines been identified and implemented?	**ID.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.	
MIL3-Managed	1.	Is there management oversight of the performance of the asset management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform asset management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform asset management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are asset management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of asset management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to asset management activities documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment	NIST CSF References	Notes
	2 Controls Management The purpose of Controls Management is to identify, analyze, and manage controls in a critical service's operating environment.		
	Goal 1—Control objectives are established.		
1.	Have control objectives been established for assets (technology, information, facilities, and people) required for delivery of the critical service? [CTRL:SG1.SP1] *People* *Information* *Technology* *Facilities*	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **PR.PT:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	The concept of objectives relates to most of the subcategories in the PROTECT category. PR.AT is mapped to the CRR Training and Awareness domain.
2.	Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA**: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **PR.PT**: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
	Goal 2—Controls are implemented.		
1.	Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **PR.PT:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	The concept of controls and control objectives apply to the broader categories in addition to the specific subcategories listed.
2.	Have controls been implemented, incorporating network segregation where appropriate, to protect network integrity? [CTRL:SG2.SP1]	**PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate.	
3.	Have controls been implemented to protect data-at-rest? [CTRL:SG2.SP1][KIM.SG4.SP2]	**PR.DS-1:** Data-at-rest is protected	
4.	Have controls been implemented to protect data-in-transit? [CTRL:SG2.SP1][KIM.SG4.SP1] [KIM:SG4.SP2]	**PR.DS-2:** Data-in-transit is protected	

	CRR Self-Assessment		NIST CSF References	Notes
	5.	Have controls been implemented to protect against data leaks? [CTRL:SG2.SP1] [KIM:SG4.SP1][KIM:SG4.SP2]	**PR.DS-5:** Protections against data leaks are implemented	
	6.	Have audit/log records been determined, documented, implemented, and reviewed in accordance with policy? [CTRL:SG2.SP1] [MON:SG1.SP3]	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	
	7.	Have controls been implemented to protect and restrict the use of removable media in accordance with policy? [CTRL:SG2.SP1] [TM:SG2.SP2]	**PR.PT-2:** Removable media is protected and its use restricted according to policy	
	8.	Have controls been implemented to protect communication and control networks? [CTRL:SG2.SP1][TM:SG2.SP2]	**PR.PT-4:** Communications and control networks are protected	
	9.	Have cybersecurity human resource practices been implemented for the critical service (e.g., de-provisioning, personnel screening)? [CTRL:SG2.SP1][HRM:SG3.SP1]	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	10.	Is access to systems and assets controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting, etc.)? [CTRL:SG2.SP1][TM:SG2.SP2]	**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality	
	Goal 3—Control designs are analyzed to ensure they satisfy control objectives.			
	1.	Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1]	**PR.IP-7:** Protection processes are continuously improved	
		People		
		Information		
		Technology		
		Facilities		
	2.	As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]	**PR.IP-7:** Protection processes are continuously improved	
	Goal 4—The internal control system is assessed to ensure control objectives are met.			
	1.	Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]	**PR.IP-7:** Protection processes are continuously improved	
		People		
		Information		
		Technology		
		Facilities		
	2.	As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]	**PR.IP-7:** Protection processes are continuously improved	
MIL2-Planned	1.	Is there a plan for performing controls management activities?	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **PR.PT**: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	

	CRR Self-Assessment		NIST CSF References	Notes
MIL2-Planned	2.	Is there a documented policy for controls management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for controls management activities have been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have controls management standards and guidelines been identified and implemented?	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. **PR.PT**: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
MIL3-Managed	1.	Is there management oversight of the performance of the controls management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform controls management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform controls management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are controls management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of controls management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of controls management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to controls management documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment	NIST CSF References	Notes
	3 Configuration and Change Management The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits.		
	Goal 1—The life cycle of assets is managed.		
	1. Is a change management process used to manage modifications to assets? [ADM:SG3.SP2] *Information* *Technology* *Facilities*	**PR.IP-3**: Configuration change control processes are in place	
	2. Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3] *Information* *Technology* *Facilities*	**PR.IP-3:** Configuration change control processes are in place	
	3. Is capacity management and planning performed for assets? [TM:SG5.SP3]	**PR.DS-4:** Adequate capacity to ensure availability is maintained	
	4. Are change requests tracked to closure? [TM:SG4.SP3]	**PR.IP-3:** Configuration change control processes are in place	
	5. Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	**PR.IP-3:** Configuration change control processes are in place	
	6. Is a System Development Life Cycle implemented to manage systems supporting the critical service? [ADM:SG3.SP2][RTSE:SG2.SP2]	**PR.IP-2**: A System Development Life Cycle to manage systems is implemented	
	Goal 2—The integrity of technology and information assets is managed.		
	1. Is configuration management performed for technology assets? [TM:SG4.SP2]	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	
	2. Are techniques in use to detect changes to technology assets? [TM:SG4.SP3]	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	
	3. Are modifications to technology assets reviewed? [TM:SG4.SP3][TM:SG4.SP2]	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained **PR.IP-3:** Configuration change control processes are in place	
	4. Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1]	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties **PR.IP-3:** Configuration change control processes are in place **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	5. Is the integrity of information assets monitored? [KIM:SG5.SP3]	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	
	6. Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2][TM:SG4.SP3]	**PR.IP-3:** Configuration change control processes are in place	
	7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	**PR.DS-7:** The development and testing environment(s) are separate from the production environment	
	8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	
	9. Is the maintenance and repair of assets performed and logged in a timely manner? [ADM:SG3.SP2][TM:SG5.SP2]	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	
	10. Is the maintenance and repair of assets performed with approved and controlled tools and/or methods? [ADM:SG3.SP2][TM:SG5.SP2]	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	

	CRR Self-Assessment		NIST CSF References	Notes
	11.	Is the remote maintenance and repair of assets approved, logged, and performed in a manner that prevents unauthorized access? [ADM:SG3.SP2][TM:SG5.SP2]	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	
	Goal 3—Asset configuration baselines are established.			
	1.	Do technology assets have configuration baselines? [TM:SG4.SP2]	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	
	2.	Is approval obtained for proposed changes to baselines? [TM:SG4.SP3]	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained **PR.IP-3:** Configuration change control processes are in place	
	3.	Has a baseline of network operations been established? [TM:SG4.SP2]	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
	4.	Is the baseline of network operations managed? [TM:SG4.SP2]	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
	5.	Has a baseline of expected data flows for users and systems been established? [TM:SG4.SP2]	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
	6.	Is the baseline of expected data flows for users and systems managed? [TM:SG4.SP2]	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
MIL2-Planned	1.	Is there a documented plan for performing change management activities?	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	
	2.	Is there a documented policy for change management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for change management activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have change management standards and guidelines been identified and implemented?	**PR.AC:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. **PR.DS:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. **PR.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.MA:** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	

	CRR Self-Assessment		NIST CSF References	Notes
MIL3-Managed	1.	Is there management oversight of the performance of the change management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform change management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform change management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6**: Risk responses are identified and prioritized	
MIL4-Measured	1.	Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are change management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of change management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of change management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to change management documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment	NIST CSF References	Notes
	4 Vulnerability Management The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.		
	Goal 1—Preparation for vulnerability analysis and resolution activities is conducted.		
1.	Has a vulnerability analysis and resolution strategy been developed? [VAR:SG1.SP2] *People* *Information* *Technology* *Facilities*	**PR.IP-12:** A vulnerability management plan is developed and implemented	
2.	Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR:SG1.SP2] *People* *Information* *Technology* *Facilities*	**DE.CM**: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	
3.	Is there a standard set of tools and/or methods in use to detect malicious code in assets? [VAR:SG1.SP2]	**DE.CM-4:** Malicious code is detected	
4.	Is there a standard set of tools and/or methods in use to detect unauthorized mobile code in assets? [VAR:SG1.SP2]	**DE.CM-5:** Unauthorized mobile code is detected	
5.	Is there a standard set of tools and/or methods in use to monitor assets for unauthorized personnel, connections, devices, and software? [VAR:SG1.SP2]	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	
	Goal 2—A process for identifying and analyzing vulnerabilities is established and maintained.		
1.	Have sources of vulnerability information been identified? [VAR:SG2.SP1] *Information* *Technology* *Facilities*	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources	
2.	Is the information from these sources kept current? [VAR:SG2.SP1] *Information* *Technology* *Facilities*	**DE.DP-5:** Detection processes are continuously improved **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **PR.IP-7**: Protection processes are continuously improved	DE.DP-5 points to NIST SP 800-53 Rev. 4 RA-5 which encompasses vulnerability scanning.
3.	Are vulnerabilities being actively discovered? [VAR:SG2.SP2] *Information* *Technology* *Facilities*	**DE.CM-8:** Vulnerability scans are performed **ID.RA-1:** Asset vulnerabilities are identified and documented	
4.	Are vulnerabilities categorized and prioritized? [VAR:SG2.SP3] *Information* *Technology* *Facilities*	**PR.IP-12:** A vulnerability management plan is developed and implemented	
5.	Are vulnerabilities analyzed to determine relevance to the organization? [VAR:SG2.SP3] *Information* *Technology* *Facilities*	**PR.IP-12:** A vulnerability management plan is developed and implemented	

	CRR Self-Assessment		NIST CSF References	Notes
	6.	Is a repository used for recording information about vulnerabilities and their resolution? [VAR:SG2.SP2] *Information* *Technology* *Facilities*	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented	
	Goal 3—Exposure to identified vulnerabilities is managed.			
	1.	Are actions taken to manage exposure to identified vulnerabilities? [VAR:SG3.SP1]	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	
	2.	Is the effectiveness of vulnerability mitigation reviewed? [VAR:SG3.SP1]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7:** Protection processes are continuously improved **RS.IM:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
	3.	Is the status of unresolved vulnerabilities monitored? [VAR:SG3.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented	
	Goal 4—The root causes of vulnerabilities are addressed.			
	1.	Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR:SG4.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented **RS.IM:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
MIL2-Planned	1.	Is there a documented plan for performing vulnerability management activities?	**PR.IP-12:** A vulnerability management plan is developed and implemented	
	2.	Is there a documented policy for vulnerability management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for vulnerability management activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have vulnerability management standards and guidelines been identified and implemented?	**PR.IP-12:** A vulnerability management plan is developed and implemented	
MIL3-Managed	1.	Is there management oversight of the performance of the vulnerability management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform vulnerability management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform vulnerability management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned vulnerability management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	

	CRR Self-Assessment		NIST CSF References	Notes
MIL4-Measured	1.	Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of vulnerability management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of vulnerability management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to vulnerability management activities documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment		NIST CSF References	Notes
	5 Incident Management The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response.			
	Goal 1—A process for identifying, analyzing, responding to, and learning from incidents established.			
	1.	Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	2.	Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-10:** Response and recovery plans are tested	
	3.	Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	4.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **RS.CO-1:** Personnel know their roles and order of operations when a response is needed	
	Goal 2—A process for detecting, reporting, triaging, and analyzing events established.			
	1.	Are events detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)? [IMC:SG2.SP1]	**DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **DE.DP-4:** Event detection information is communicated to appropriate parties **RS.CO-2:** Events are reported consistent with established criteria	
	2.	Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]	**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors	
	3.	Are events categorized? [IMC:SG2.SP4]	**RS.AN-4:** Incidents are categorized consistent with response plans	
	4.	Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors	
	5.	Are events prioritized? [IMC:SG2.SP4]	**DE.AE-4:** Impact of events is determined	
	6.	Is the status of events tracked? [IMC:SG2.SP4]	**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors	
	7.	Are events tracked to resolution? [IMC:SG2.SP4]	**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors **RS.AN-1:** Notifications from detection systems are investigated	
	8.	Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]	**DE.DP-2:** Detection activities comply with all applicable requirements **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
	9.	Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **RS.AN-3:** Forensics are performed	

		CRR Self-Assessment	NIST CSF References	Notes
	Goal 3—Incidents are declared and analyzed.			
	1.	Are incidents declared? [IMC:SG3.SP1]	**RS.CO-2:** Events are reported consistent with established criteria	
	2.	Have criteria for the declaration of an incident been established? [IMC.SG3.SP1]	**DE.AE-5:** Incident alert thresholds are established	
	3.	Are incidents analyzed to determine a response? [IMC:SG3.SP2]	**RS.AN-2:** The impact of the incident is understood **RS.AN-4:** Incidents are categorized consistent with response plans	
	Goal 4—A process for responding to and recovering from incidents is established.			
	1.	Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	
	2.	Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]	**RS.MI-1:** Incidents are contained **RS.RP-1:** Response plan is executed during or after an event	
	3.	Are incident status and response communicated to affected parties (including public relations staff and external media outlets)? [IMC:SG4.SP3]	**RC.CO-1:** Public Relations are managed **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams **RS.CO-3:** Information is shared consistent with response plans	
	4.	Are incidents tracked to resolution? [IMC:SG4.SP4]	**RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated	
	Goal 5—Post-incident lessons learned are translated into improvement strategies.			
	1.	Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7:** Protection processes are continuously improved	
	2.	Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7:** Protection processes are continuously improved	
	3.	Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7**: Protection processes are continuously improved **RS.IM-1:** Response plans incorporate lessons learned **RS.IM-2:** Response strategies are updated	
MIL2-Planned	1.	Is there a documented plan for performing incident management activities?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	2.	Is there a documented policy for incident management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for incident management activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have incident management standards and guidelines been identified and implemented?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	

	CRR Self-Assessment		NIST CSF References	Notes
MIL3-Managed	1.	Is there management oversight of the performance of the incident management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform incident management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform incident management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned incident management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**DE.DP-3:** Detection processes are tested **PR.IP-7:** Protection processes are continuously improved	
	2.	Are incident management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of incident management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of incident management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to incident management activities documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment	NIST CSF References	Notes
	6 Service Continuity Management The purpose of Service Continuity Management is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.		
	Goal 1—Service continuity plans for high-value services are developed.		
	1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2] *People* *Information* *Technology* *Facilities*	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **RS.CO-1:** Personnel know their roles and order of operations when a response is needed	
	4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	
	5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	Goal 2—Service continuity plans are reviewed to resolve conflicts between plans.		
	1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **RC.IM:** Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Goal 3 - Service continuity plans tested to ensure they meet their stated objectives.		
	1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	**PR.IP-10:** Response and recovery plans are tested	
	2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	**PR.IP-10:** Response and recovery plans are tested	
	3. Are service continuity plans tested? [SC:SG5.SP3]	**PR.IP-10:** Response and recovery plans are tested	
	4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically	
	5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	**PR.IP-10:** Response and recovery plans are tested **RC.IM:** Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Goal 4—Service continuity plans are executed and reviewed.		
	1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **RC.RP-1:** Recovery plan is executed during or after an event	

	CRR Self-Assessment		NIST CSF References	Notes
	2.	Is the execution of service continuity plans reviewed? [SC:SG6.SP2]	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **RC.IM:** Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	3.	Are improvements identified as a result of executing service continuity plans? [SC:SG7.SP2]	**RC.IM-1:** Recovery plans incorporate lessons learned **RC.IM-2**: Recovery strategies are updated	
MIL2-Planned	1.	Is there a documented plan for performing service continuity activities?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	2.	Is there a documented policy for service continuity?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for service continuity activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have service continuity standards and guidelines been identified and implemented?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
MIL3-Managed	1.	Is there management oversight of the performance of the service continuity activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform service continuity activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform service continuity activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are service continuity activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7**: Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of service continuity?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of service continuity activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to service continuity documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment		NIST CSF References	Notes
	7 Risk Management The purpose of Risk Management is to identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.			
	Goal 1—A strategy for identifying, analyzing, and mitigating risks is developed.			
	1.	Have sources of risk that can affect operations been identified? [RISK:SG1.SP1]	**ID.RM:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	2.	Have categories been established for risks? [RISK:SG1.SP1]	**ID.RM**: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	3.	Has a plan for managing operational risk been established? [RISK:SG1.SP2]	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
	4.	Is the plan for managing operational risk communicated to stakeholders? [RISK:SG1.SP2]	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
	Goal 2—Risk tolerances are identified, and the focus of risk management is established.			
	1.	Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK:SG2.SP2]	**ID.RA-4:** Potential business impacts and likelihoods are identified **RC.CO-2:** Reputation after an event is repaired	
	2.	Have impact areas been prioritized to determine their relative importance? [RISK:SG2.SP2]	**ID.RA-4:** Potential business impacts and likelihoods are identified **ID.RM:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	3.	Have risk tolerance parameters been established for each impact area? [RISK:SG2.SP2]	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed **ID.RM-3:** The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	
	4.	Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK:SG2.SP1]	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed **ID.RM-3:** The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis **RC.CO-2:** Reputation after an event is repaired	
	Goal 3—Risks are identified.			
	1.	Are operational risks that could affect delivery of the critical service identified? [RISK:SG3.SP2]	**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	
	Goal 4—Risks are analyzed and assigned a disposition.			
	1.	Are risks analyzed to determine potential impact to the critical service [RISK:SG4.SP1]?	**ID.RA-4:** Potential business impacts and likelihoods are identified	
	2.	Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK:SG4.SP3]	**ID.RA-6:** Risk responses are identified and prioritized	
	Goal 5—Risks to assets and services are mitigated and controlled.			
	1.	Are plans developed for risks that the organization decides to mitigate? [RISK:SG5.SP1]	**ID.RA-6:** Risk responses are identified and prioritized **ID.RM:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	2.	Are identified risks tracked to closure? [RISK:SG5.SP2]	**ID.RA-6:** Risk responses are identified and prioritized **ID.RM:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	

	CRR Self-Assessment		NIST CSF References	Notes
MIL2-Planned	1.	Is there a documented plan for performing risk management activities?	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
	2.	Is there a documented policy for risk management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for risk management activities have identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have risk management activities standards and guidelines been identified and implemented?	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
MIL3-Managed	1.	Is there management oversight of the performance of the risk management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform risk management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform risk management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are risk management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7:** Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of risk management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of risk management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to risk management documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment		NIST CSF References	Notes
	8 External Dependencies Management The purpose of External Dependencies Management is to establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.			
	Goal 1—External dependencies are identified and prioritized to ensure sustained operation of high-value services.			
	1.	Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
	2.	Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
	3.	Are external dependencies prioritized? [EXD:SG1.SP2]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
	Goal 2—Risks due to external dependencies are identified and managed.			
	1.	Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ID.BE-1 guidance (SA-12 in NIST 800-53) contains subpractices that mainly relate to supplier management.
	Goal 3—Relationships with external entities formally established and maintained.			
	1.	Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.BE-5:** Resilience requirements to support delivery of critical services are established	ID.BE-1 guidance (SA-12 in NIST 800-53) contains subpractices that mainly relate to supplier management.
	2.	Are these requirements reviewed and updated? [EXD:SG3.SP2]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.BE-5:** Resilience requirements to support delivery of critical services are established	
	3.	Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.BE-5:** Resilience requirements to support delivery of critical services are established	
	4.	Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.BE-5:** Resilience requirements to support delivery of critical services are established **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	
	Goal 4—Performance of external entities is managed.			
	1.	Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]	**DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **ID.BE-1:** The organization's role in the supply chain is identified and communicated	ID.BE-1 guidance (SA-12 in NIST 800-53) contains subpractices that mainly relate to supplier management.
	2.	Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.BE-1:** The organization's role in the supply chain is identified and communicated	
	3.	Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	NIST SP 800-53 SA-12.15 "Processes to address weaknesses or deficiencies."
	4.	Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	NIST SP 800-53 SA-12.15 "Processes to address weaknesses or deficiencies."

		CRR Self-Assessment	NIST CSF References	Notes
	Goal 5—Dependencies on public services and infrastructure service providers are identified.			
	1.	Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
	2.	Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	
MIL2-Planned	1.	Is there a documented plan for performing external dependency management activities?	**ID.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.	Many of the NIST informative references for this category relate to vendor management.
	2.	Is there a documented policy for external dependency management?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for external dependency management activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have external dependency management activities standards and guidelines been identified and implemented?	**ID.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.	
MIL3-Managed	1.	Is there management oversight of the performance of the external dependency management activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform external dependency management activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform external dependency management activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned external dependency management activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risk **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results.	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are external dependency management activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7**: Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to external dependency management?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of the external dependency management activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to external dependency management documented and shared across the organization?	**PR.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.	

		CRR Self-Assessment	NIST CSF References	Notes
	9 Training and Awareness The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.			
	Goal 1—Cyber security awareness and training programs are established.			
	1.	Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	**PR.AT-1:** All users are informed and trained	
	2.	Have required cyber security skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP1]	**PR.AT-1:** All users are informed and trained	
	3.	Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]	**PR.AT-1:** All users are informed and trained	
	4.	Have cyber security training needs been identified? [OTA:SG3.SP1]	**PR.AT-1:** All users are informed and trained	
	Goal 2—Awareness and training activities are conducted.			
	1.	Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]	**PR.AT-1:** All users are informed and trained	
	2.	Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	**PR.AT-1**: All users are informed and trained	
	3.	Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	**PR.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.IP-7:** Protection processes are continuously improved	
	4.	Are awareness and training activities revised as needed? [OTA:SG1.SP3][OTA:SG3.SP3]	**PR.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.IP-7:** Protection processes are continuously improved	
	5.	Have privileged users been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	**PR.AT-2:** Privileged users understand roles & responsibilities	
	6.	Have senior executives been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	**PR.AT-4:** Senior executives understand roles & responsibilities	
	7.	Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities	
MIL2-Planned	1.	Is there a documented plan for performing training activities?	**PR.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.	
	2.	Is there a documented policy for training?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for training activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have training standards and guidelines been identified and implemented?	**PR.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.	

	CRR Self-Assessment		NIST CSF References	Notes
MIL3-Managed	1.	Is there management oversight of the performance of the training activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform training activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform training activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are training activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are training activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7**: Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to the performance of training?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to training documented and shared across the organization?	**PR.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.	

	CRR Self-Assessment		NIST CSF References	Notes
	10 Situational Awareness The purpose of Situational Awareness is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.			
	Goal 1—Threat monitoring is performed.			
	1.	Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **PR.AT-5:** Physical and information security personnel understand roles & responsibilities	
	2.	Have threat monitoring procedures been implemented? [MON:SG2.SP2]	**ID.RA-3:** Threats, both internal and external, are identified and documented	
	3.	Have resources been assigned to threat monitoring processes? [MON:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities	
	Goal 2—The requirements for communicating threat information are established.			
	1.	Have internal stakeholders (such as the critical service owner and incident management staff) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	Goal 3—Threat information is communicated.			
	1.	Is threat information communicated to stakeholders? [COMM:SG3.SP2]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	2.	Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities	
	3.	Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	**PR.AT-1:** All users are informed and trained **PR.AT-5:** Physical and information security personnel understand roles & responsibilities	PR.AT-5 Guidance -NIST 800-53 AT-3 points to role based-security training.
MIL2-Planned	1.	Is there a documented plan for performing situational awareness activities?	**ID.RA**: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	2.	Is there a documented policy for situational awareness?	**ID.GV-1:** Organizational information security policy is established **PR.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.	
	3.	Have stakeholders for situational awareness activities been identified and made aware of their roles?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners **PR.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.	
	4.	Have situational awareness standards and guidelines been identified and implemented?	**ID.RA**: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	

	CRR Self-Assessment		NIST CSF References	Notes
MIL3-Manaed	1.	Is there management oversight of the performance of situational awareness activities?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
	2.	Have qualified staff been assigned to perform situational awareness activities as planned?	**PR.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.	
	3.	Is there adequate funding to perform situational awareness activities as planned?	**ID.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.	The concept of funding is not directly addressed in the CSF. Funding should come from the decisions and activities mentioned within category ID.BE.
	4.	Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-6:** Risk responses are identified and prioritized	
MIL4-Measured	1.	Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results?	**PR.IP-7:** Protection processes are continuously improved	
	2.	Are situational awareness activities periodically reviewed to ensure they are adhering to the plan?	**PR.IP-7**: Protection processes are continuously improved	
	3.	Is higher-level management aware of issues related to situational awareness?	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	
MIL5-Defined	1.	Has the organization adopted a standard definition of the situational awareness activities from which operating units can derive practices that fit their unique operating circumstances?	**PR.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.	The PR.IP category broadly covers security policies, processes, and procedures for the protection of services and related assets.
	2.	Are improvements to situational awareness activities documented and shared across the organization?	**PR.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.	

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
MIL	CRR Maturity Indicator Level

References	
CRR	http://www.us-cert.gov/ccubedvp/self-service-crr
RMM	http://www.cert.org/resilience/products-services/cert-rmm/index.cfm

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
RRM	Resilience Requirements Management
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

* RMM references for the CRR questions can be found in the CRR to CSF Crosswalk starting on page 13.

This page is intentionally blank.

Homeland Security