CISA
CYBER+INFRASTRUCTURE

EXTERNAL DEPENDENCIES MANAGEMENT (EDM)

NIST Cybersecurity Framework Crosswalks

April 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

DM19-0492

Contents

NIST Cybersecurity Framework (CSF) to External Dependencies Management Assessment (EDM) Crosswalk 1
Identify (ID) 2
Protect (PR) 5
Detect (DE) 9
Respond (RS) 11
Recover (RC) 13
Crosswalk Reference Key 14

External Dependencies Management Assessment (EDM) to NIST Cybersecurity Framework (CSF) Crosswalk 15
1 Relationship Formation 16
2 Relationship Management and Governance 19
3 Service Protection and Sustainment 24
Crosswalk Reference Key 27

NIST Cybersecurity Framework (CSF) to External Dependencies Management Assessment (EDM) Crosswalk

Function	Category	Subcategory	EDM 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 organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried**	RF:G1.Q3***	• CIS 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, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	RF:G1.Q3	• CIS 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, A.12.5.1 • NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	N/A. Please see footnote on Page 2.****	• CIS CSC 12 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	RF:G1.Q3	• CIS CSC 12 • COBIT 5 APO02.02, APO10.04, DSS01.02 • 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, time, personnel, and software) are prioritized based on their classification, criticality, and business value	RF:G1.Q2	• CIS CSC 13, 14 • COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, 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, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	RMG:G6.Q2 RMG:G6.Q3 SPS:G3.Q1	• CIS CSC 17, 19 • COBIT 5 APO01.02, APO07.06, APO13.01, 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. **EDM References** RF:G1.Q1 RF:G1.Q2	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	RF:G2.Q1 RF:G2.Q2 RF:G2.Q3 RF:G2.Q4 RF:G3.Q2-S RF:G3.Q2-IP RF:G3.Q2-G RF:G4.Q2 RF:G5.Q1 RMG:G2.Q1 RMG:G6.Q1	• COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, 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	N/A. Please see footnote on Page 2.****	• COBIT 5 APO02.06, APO03.01 • ISO/IEC 27001:2013 Clause 4.1 • NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	N/A. Please see footnote on Page 2.****	• 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	RF:G2.Q4 RF:G4.Q2 RF:G6.Q2 RMG:G1.Q1-S RMG:G1.Q1-IP RMG:G1.Q1-G RMG:G1.Q2 RMG:G1.Q3	• COBIT 5 APO10.01, BAI04.02, BAI09.02 • 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 for all operating states (e.g. under duress/attack, during recovery, normal operations)	RF:G1.Q4 RF:G2.Q3 RF:G6.Q1 RMG:G2.Q1 RMG:G6.Q1	• COBIT 5 BAI03.02, 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-13, SA-14

* RMM references for the EDM questions can be found in the EDM to CSF Crosswalk starting on page 15.
** Denotes NIST CSF Reference with format of [NIST CSF Function.Category-Subcategory Number].
*** Denotes EDM reference with format of [EDM Domain:Goal.Question-External Entity type(s) (S,IP,G), Asset type(s) (I,T,F,P), or Continuity plans (IM,SC)].
**** The External Dependencies Management Assessment (EDM) has as its focus external dependency risk (aka supply chain risk), and as such is not designed to directly map to all of the Cybersecurity Framework (CSF) categories or sub-categories. A companion product, the Cyber Resilience Review (CRR) which is intended as a comprehensive cybersecurity assessment tool, does map to all of the CSF.

Function	Category	Subcategory	EDM 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 cybersecurity policy is established and communicated	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 APO01.03, APO13.01, 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 security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	RMG:G6.Q2 RMG:G6.Q3	• CIS CSC 19 • COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 • NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	RF:G1.Q4 RF:G2.Q2	• CIS CSC 19 • COBIT 5 BAI02.01, MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7 • ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 • NIST SP 800-53 Rev. 4 -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	RF:G3.Q1	• COBIT 5 EDM03.02, APO12.02, APO12.05, 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 • ISO/IEC 27001:2013 Clause 6 • NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	RF:G6.Q2 RMG:G2.Q4	• CIS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 • 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: Cyber threat intelligence is received from information sharing forums and sources	SPS:G3.Q1 SPS:G3.Q2 SPS:G3.Q4 SPS:G3.Q5	• CIS CSC 4 • COBIT 5 BAI08.01 • 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 SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented	SPS:G3.Q2 SPS:G3.Q3-S SPS:G3.Q3-IP	• CIS CSC 4 • 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 • ISO/IEC 27001:2013 Clause 6.1.2 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	RF:G3.Q3	• CIS CSC 4 • COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 • NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RF:G3.Q2-S RF:G3.Q2-G RF:G3.Q2-IP RF:G3.Q3	• CIS CSC 4 • COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

Function	Category	Subcategory	EDM References	Informative References
Identify (ID)		**ID.RA-6:** Risk responses are identified and prioritized	RF:G3.Q2-S RF:G3.Q2-IP RF:G3.Q2-G	• CIS CSC 4 • COBIT 5 APO12.05, APO13.02 • ISO/IEC 27001:2013 Clause 6.1.3 • NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	RF:G3.Q1 RMG:G2.Q5 RMG:G2.Q6 RMG:G6.Q5	• CIS CSC 4 • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISA 62443-2-1:2009 4.3.4.2 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 • NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 • NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 • NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	RF:G2.Q1 RF:G3.Q1 RF:G3.Q2-S RF:G3.Q2-IP RF:G3.Q2-G RMG:G2.Q2 RMG:G2.Q5 RMG:G2.Q6 RMG:G3.Q2 RMG:G4.Q3 RMG:G4.Q4 RMG:G5.Q1 RMG:G5.Q2 RMG:G5.Q3 RMG:G6.Q5 SPS:G2.Q4	• CIS CSC 4 • COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • ISA 62443-2-1:2009 4.3.4.2 • ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	RF:G2.Q1 RF:G3.Q2-S RF:G3.Q2-IP RF:G3.Q2 -G RF:G3.Q3 RF:G4.Q1 RF:G4.Q3 RF:G4.Q4 RF:G6.Q3 RF:G6.Q4 RF:G6.Q5 RMG:G1.Q1-S RMG:G1.Q1-IP RMG:G1.Q1-G RMG:G1.Q2 RMG:G1.Q3 RMG:G2.Q3 RMG:G2.Q5 RMG:G2.Q6 SPS:G1.Q4-IM SPS:G1.Q4-SC SPS:G2.Q2-IM SPS:G2.Q2-SC SPS:G2.Q4	• COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 • ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	RF:G2.Q1 RF:G2.Q2 RF:G2.Q3 RF:G2.Q4 RF:G4.Q1 RF:G4.Q2 RF:G4.Q3 RF:G4.Q4 RF:G5.Q1 RF:G5.Q2 RF:G5.Q3 RF:G5.Q4 RF:G5.Q5 RF:G5.Q6 RMG:G2.Q1 RMG:G4.Q3 RMG:G4.Q5 RMG:G5.Q1 RMG:G5.Q2 RMG:G6.Q1 SPS:G2.Q2-IM SPS:G2.Q2-SC SPS:G2.Q4	• COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 • ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 • NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	RF:G3.Q2-S RF:G3.Q2-IP RF:G3.Q2-G RF:G3.Q3 RMG:G2.Q2 RMG:G2.Q3 RMG:G2.Q4 RMG:G2.Q5 RMG:G2.Q6 RMG:G3.Q1 RMG:G3.Q2 RMG:G3.Q3 RMG:G3.Q4 RMG:G4.Q3 RMG:G4.Q4 RMG:G4.Q5 RMG:G6.Q2 RMG:G6.Q3 RMG:G6.Q4 SPS:G2.Q1-IM SPS:G2.Q1-SC SPS:G2.Q3 SPS:G2.Q4	• COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • ISA 62443-2-1:2009 4.3.2.6.7 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

Function	Category	Subcategory	EDM References			Informative References
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	RF:G5.Q6 SPS:G1.Q1 SPS:G1.Q3	SPS:G1.Q4-IM SPS:G1.Q4-SC SPS:G1.Q5-IM	SPS:G1.Q5-SC SPS:G2.Q1-IM SPS:G2.Q1-SC	• CIS CSC 19, 20 • COBIT 5 DSS04.04 • ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR 6.1, SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
Protect (PR)	**Identity Management, Authentication and Access Control (AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	RMG:G7.Q1 RMG:G7.Q2 RMG:G7.Q3-I	RMG:G7.Q3-T RMG:G7.Q3-F RMG:G7.Q4-I	RMG:G7.Q4-T RMG:G7.Q4-F	• CIS CSC 1, 5, 15, 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.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	RMG:G7.Q1 RMG:G7.Q2 RMG:G7.Q3-I	RMG:G7.Q3-T RMG:G7.Q3-F RMG:G7.Q4-I	RMG:G7.Q4-T RMG:G7.Q4-F	• 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.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	RMG:G7.Q1 RMG:G7.Q2 RMG:G7.Q3-I	RMG:G7.Q3-T RMG:G7.Q3-F RMG:G7.Q4-I	RMG:G7.Q4-T RMG:G7.Q4-F	• CIS CSC 12 • 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.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	RMG:G7.Q3-I RMG:G7.Q3-T RMG:G7.Q3-F			• CIS CSC 3, 5, 12, 14, 15, 16, 18 • COBIT 5 DSS05.04 • 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, A.9.4.5 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	N/A. Please see footnote on Page 2.****			• CIS CSC 9, 14, 15, 18 • COBIT 5 DSS01.05, DSS05.02 • 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, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	RMG:G7.Q1			• CIS CSC, 16 • COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 • ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

Function	Category	Subcategory	EDM References	Informative References
Protect (PR)		**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	RMG:G7.Q1	• CIS CSC 1, 12, 15, 16 • COBIT 5 DSS05.04, DSS05.10, DSS06.10 • ISA 62443-2-1:2009 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 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	N/A. Please see footnote on Page 2.****	• CIS CSC 17, 18 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 • NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	N/A. Please see footnote on Page 2.****	• CIS CSC 5, 17, 18 • COBIT 5 APO07.02, DSS05.04, 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
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	RF:G5.Q1	• CIS CSC 17 • COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	N/A. Please see footnote on Page 2.****	• CIS CSC 17, 19 • COBIT 5 EDM01.01, APO01.02, 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 cybersecurity personnel understand their roles and responsibilities	SPS:G3.Q1	• CIS CSC 17 • 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, IR-2, PM-13
	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	N/A. Please see footnote on Page 2.****	• CIS CSC 13, 14 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, 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 MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	N/A. Please see footnote on Page 2.****	• CIS CSC 13, 14 • COBIT 5 APO01.06, DSS05.02, 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, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	N/A. Please see footnote on Page 2.****	• CIS CSC 1 • COBIT 5 BAI09.03 • ISA 62443-2-1:2009 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.11.2.5, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16

Function	Category	Subcategory	EDM References	Informative References
Protect (PR)		**PR.DS-4:** Adequate capacity to ensure availability is maintained	RMG:G4.Q5	• CIS CSC 1, 2, 13 • COBIT 5 APO13.01, BAI04.04 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	N/A. Please see footnote on Page 2.****	• CIS CSC 13 • COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 • 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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, 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	N/A. Please see footnote on Page 2.****	• CIS CSC 2, 3 • COBIT 5 APO01.06, BAI06.01, DSS06.02 • 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, A.14.2.4 • NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	N/A. Please see footnote on Page 2.****	• CIS CSC 18, 20 • COBIT 5 BAI03.08, BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	N/A. Please see footnote on Page 2.****	• COBIT 5 BAI03.05 • ISA 62443-2-1:2009 4.3.4.4.4 • ISO/IEC 27001:2013 A.11.2.4 • NIST SP 800-53 Rev. 4 SA-10, SI-7
	Information Protection Processes and Procedures (IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	N/A. Please see footnote on Page 2.****	• CIS CSC 3, 9, 11 • 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	RF:G6.Q5 RMG:G5.Q1	• CIS CSC 18 • COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 • 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 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	RMG:G4.Q1-I RMG:G4.Q2-I RMG:G4.Q1-T RMG:G4.Q2-T RMG:G4.Q1-F RMG:G4.Q2-F RMG:G4.Q1-P RMG:G4.Q2-P	• CIS CSC 3, 11 • COBIT 5 BAI01.06, BAI06.01 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 10 • COBIT 5 APO13.01, DSS01.01, DSS04.07 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

Function	Category	Subcategory	EDM References	Informative References
Protect (PR)		**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met	RF:G2.Q2 RMG:G3.Q1	• 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	N/A. Please see footnote on Page 2.****	• COBIT 5 BAI09.03, DSS05.06 • 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 improved	RMG:G5.Q3	• COBIT 5 APO11.06, APO12.06, 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 • ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	RMG:G5.Q3 SPS:G3.Q3-IP SPS:G3.Q6 SPS:G3.Q3-S SPS:G3.Q4	• COBIT 5 BAI08.04, DSS03.04 • 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	SPS:G1.Q1 SPS:G1.Q4-SC SPS:G1.Q3 SPS:G1.Q5-IM SPS:G1.Q4-IM SPS:G1.Q5-SC	• CIS CSC 19 • COBIT 5 APO12.06, 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, A.17.1.3 • NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	N/A. Please see footnote on Page 2.****	• CIS CSC 19, 20 • COBIT 5 DSS04.04 • 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)	RMG:G7.Q2	• CIS CSC 5, 16 • 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.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented	RMG:G2.Q4	• CIS CSC 4, 18, 20 • COBIT 5 BAI03.10, DSS05.01, DSS05.02 • ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	RMG:G4.Q2-I RMG:G4.Q2-F RMG:G4.Q2-T RMG:G4.Q2-P	• COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 • 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, A.11.2.6 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	RMG:G4.Q2-I RMG:G4.Q2-P RMG:G7.Q4-T RMG:G4.Q2-T RMG:G7.Q1 RMG:G7.Q4-F RMG:G4.Q2-F RMG:G7.Q4-I	• CIS CSC 3, 5 • COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4

Function	Category	Subcategory	EDM References	Informative References
Protect (PR)	**Protective Technology (PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	N/A. Please see footnote on Page 2.****	• CIS CSC 1, 3, 5, 6, 14, 15, 16 • COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 8, 13 • COBIT 5 APO13.01, DSS05.02, DSS05.06 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.1, 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-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	N/A. Please see footnote on Page 2.****	• CIS CSC 3, 11, 14 • COBIT 5 DSS05.02, DSS05.05, DSS06.06 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 8, 12, 15 • 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, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	N/A. Please see footnote on Page 2.****	• COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 • ISA 62443-2-1:2009 4.3.2.5.2 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 • NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
Detect (DE)	**Anomalies and Events (AE):** Anomalous activity is detected 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	N/A. Please see footnote on Page 2.****	• CIS CSC 1, 4, 6, 12, 13, 15, 16 • COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 3, 6, 13, 15 • COBIT 5 DSS05.07 • 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 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.12.4.1, 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 collected and correlated from multiple sources and sensors	N/A. Please see footnote on Page 2.****	• CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • COBIT 5 BAI08.02 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

Function	Category	Subcategory	EDM References	Informative References
Detect (DE)		**DE.AE-4:** Impact of events is determined	N/A. Please see footnote on Page 2.****	• CIS CSC 4, 6 • COBIT 5 APO12.06, DSS03.01 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	SPS:G1.Q2	• CIS CSC 6, 19 • COBIT 5 APO12.06, DSS03.01 • ISA 62443-2-1:2009 4.2.3.10 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	N/A. Please see footnote on Page 2.****	• CIS CSC 1, 7, 8, 12, 13, 15, 16 • COBIT 5 DSS01.03, DSS03.05, 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	N/A. Please see footnote on Page 2.****	• COBIT 5 DSS01.04, DSS01.05 • ISA 62443-2-1:2009 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 5, 7, 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 4, 7, 8, 12 • 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, SI-8
		DE.CM-5: Unauthorized mobile code is detected	N/A. Please see footnote on Page 2.****	• CIS CSC 7, 8 • COBIT 5 DSS05.01 • ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 • 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	RMG:G3.Q1 RMG:G4.Q4	• COBIT 5 APO07.06, APO10.05 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 • COBIT 5 DSS05.02, DSS05.05 • ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 • 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	RMG:G2.Q4	• CIS CSC 4, 20 • COBIT 5 BAI03.10, DSS05.01 • 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 and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 APO01.02, DSS05.01, DSS06.03 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

Function	Category	Subcategory	EDM References	Informative References
Detect (DE)		**DE.DP-2:** Detection activities comply with all applicable requirements	N/A. Please see footnote on Page 2.****	• COBIT 5 DSS06.01, MEA03.03, MEA03.04 • ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 • NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	N/A. Please see footnote on Page 2.****	• COBIT 5 APO13.02, DSS05.02 • 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, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 APO08.04, APO12.06, DSS02.05 • 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, A.16.1.3 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	N/A. Please see footnote on Page 2.****	• COBIT 5 APO11.06, APO12.06, 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 response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 APO12.06, BAI01.10 • 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 (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 EDM03.02, APO01.02, APO12.03 • 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.7.2.2, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 DSS01.03 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 DSS03.04 • ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 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
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 DSS03.04 • ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 Clause 7.4 • 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	SPS:G3.Q3-S SPS:G3.Q4 SPS:G3.Q6 SPS:G3.Q3-IP SPS:G3.Q5	• CIS CSC 19 • COBIT 5 BAI08.04 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 SI-5, PM-15

Function	Category	Subcategory	EDM References	Informative References
Respond (RS)	**Analysis (AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	N/A. Please see footnote on Page 2.****	• CIS CSC 4, 6, 8, 19 • COBIT 5 DSS02.04, 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	N/A. Please see footnote on Page 2.****	• COBIT 5 DSS02.02 • 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.16.1.4, A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Forensics are performed	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.06, DSS03.02, DSS05.07 • 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	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 DSS02.02 • 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
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	RMG:G2.Q4	• CIS CSC 4, 19 • COBIT 5 EDM03.02, DSS05.07 • NIST SP 800-53 Rev. 4 SI-5, PM-15
	Mitigation (MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	N/A. Please see footnote on Page 2.****	• CIS CSC 19 • COBIT 5 APO12.06 • 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.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	N/A. Please see footnote on Page 2.****	• CIS CSC 4, 19 • COBIT 5 APO12.06 • 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	RMG:G2.Q4	• CIS CSC 4 • COBIT 5 APO12.06 • 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.	**RS.IM-1:** Response plans incorporate lessons learned	N/A. Please see footnote on Page 2.****	• 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, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	N/A. Please see footnote on Page 2.****	• COBIT 5 BAI01.13, DSS04.08 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Function	Category	Subcategory	EDM References	Informative References
Recover (RC)	**Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	N/A. Please see footnote on Page 2.****	• CIS CSC 10 • COBIT 5 APO12.06, 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): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.06, BAI05.07, DSS04.08 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.06, BAI07.08 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	N/A. Please see footnote on Page 2.****	• COBIT 5 EDM03.02 • ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	N/A. Please see footnote on Page 2.****	• COBIT 5 MEA03.02 • ISO/IEC 27001:2013 Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	N/A. Please see footnote on Page 2.****	• COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4

Crosswalk Reference Key

External Dependencies Management Assessment (EDM) Reference Key	
F	Facilities
G	Governmental Services
G*x*	Goal
I	Information
IM	Incident Management
IP	Infrastructure Providers
MIL	Maturity Indicator Level
P	People
Q*x*	Question
RF	Relationship Formation
RMG	Relationship Management and Governance
S	Supplier
SC	Service Continuity
SPS	Service Protection and Sustainment
T	Technology

CERT® Resilience Management Model (CERT®-RMM) Reference Key*	
ADM	Asset Definition and Management
AM	Access Management
CTRL	Controls Management
EF	Enterprise Focus
EXD	External Dependencies Management
GG*x*	Generic Goal
IMC	Incident Management and Control
MON	Monitoring
RISK	Risk Management
RRM	Resilience Requirements Management
SC	Service Continuity
SG*x*	Specific Goal
SP*x*	Specific Practice
TM	Technology Management
VAR	Vulnerability Awareness and Resolution

References	
CRR	http://www.us-cert.gov/ccubedvp/self-service-crr
RMM	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

* RMM references for the EDM questions can be found in the EDM to CSF Crosswalk starting on page 15.

External Dependencies Management Assessment (EDM) to NIST Cybersecurity Framework (CSF) Crosswalk

	EDM Self-Assessment		NIST CSF References	Notes
	1 Relationship Formation The purpose of Relationship Formation is to assess whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them. Relationship Formation includes understanding the acquirer's critical services, having a process for entering into formal relationships, and evaluating external entities. A key aspect of Relationship Formation is identifying resilience requirements as the basis for risk management and formal agreements. Resilience requirements typically focus on integrity, confidentiality, and availability, but can also include other requirements important to the critical service.			
	Goal 1 - Acquirer service and asset priorities are established.			
	1.	Are the acquirer's services identified and documented across the enterprise? [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.**	
	2.	Are the acquirer's services prioritized based on an analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, 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.	Are the acquirer's assets that directly support the critical service inventoried? [ADM:SG1.SP1]	**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	
	4.	Have control objectives been established for acquirer assets that support the critical service(s)? [CTRL:SG1.SP1]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	The CRR practice concerning control objectives is mapped to all PROTECT categories other than PR.AT. The EDM is not mapped to these categories as there are controls-oriented at a level not addressed by the EDM.
	Goal 2 - Forming relationships with external entities is planned.			
	1.	Does the acquirer have an established process for entering into formal agreements with external entities? [EXD:SG3.SP3]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	2.	Has the acquirer identified and documented baseline (boilerplate) requirements that apply to any supplier that supports the critical service? [EXD:SG3.SP1]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met	PR.IP-5 is mapped to specific practices in the CRR that are not included in the EDM assessment due to its scope, focusing on supply chain risk management.
	3.	Does the acquirer have a process to identify and document resilience requirements for specific external entities (suppliers, infrastructure providers, and governmental services) that support the critical service? [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 for all operating states (e.g. under duress/attack, during recovery, normal operations) **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	4.	Does the acquirer's process to enter into formal agreements with suppliers ensure that resilience requirements are considered before entering into agreements? [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.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	

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

** Denotes NIST CSF Reference with format of [NIST CSF Function.Category-Subcategory Number].

	EDM Self-Assessment		NIST CSF References	Notes
	Goal 3 – Risk management includes external dependencies.			
	1.	Has a plan for managing operational risk been established and agreed to by Stakeholders? [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 **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	
	2.	Are the risks of relying on external entities to support the critical service identified and managed (accepted, transferred, mitigated, etc.)? [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.RA-6:** Risk responses are identified and prioritized **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	ID.RA-5 and ID.RA-6 are mapped to specific practices in the CRR related to Risk Management. The EDM assessment does not include such specific practices, but these subcategories are informed by this EDM practice.
		2.1 Suppliers		
		2.2 Infrastructure providers		
		2.3 Governmental services		
	3.	Does the acquirer identify and manage the risk of an external entity being a single point of failure? [EXD:SG1.SP2]	**ID.RA-4:** Potential business impacts and likelihoods are identified **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	Goal 4 – External entities are evaluated.			
	1.	Are resilience requirements included in written communications with prospective suppliers, for example in requests for proposals (RFPs)? [EXD:SG3.SP3]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	2.	Does the acquirer consider the ability of suppliers to meet the resilience requirements of the critical service before entering into formal agreements? [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.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	3.	Does the acquirer identify suppliers from which it requires documented verification of an ability to meet the critical service's resilience requirements? [EXD:SG3.SP3]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	4.	Does the acquirer consider external entities' own external dependency risks before entering into agreements to support the critical service? [EXD:SG3.SP3]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	

	EDM Self-Assessment		NIST CSF References	Notes
	Goal 5 – Formal agreements include resilience requirements.			
	1.	Are resilience requirements for the critical service included in formal agreements with suppliers? [EXD:SG3.SP4]	**ID.BE-1:** The organization's role in the supply chain is identified and communicated **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	
	2.	Do formal agreements require suppliers to manage their own external dependencies? [EXD:SG3.SP4, EXD:GG2.GP4]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	3.	Do formal agreements with suppliers include requirements to report incidents that affect the critical service? [EXD:SG3.SP4, IMC:GG2.GP4]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	4.	Do formal agreements require that suppliers manage vulnerabilities that may affect the critical service? [EXD:SG3.SP2, VAR:GG2.GP4]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	5.	Do formal agreements require that suppliers maintain disruption management plans (incident management, service continuity, etc.)? [IMC:GG2.GP4, SC:GG2.GP4]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	6.	Do formal agreements with suppliers that support the critical service require their participation in disruption management planning and exercising? [IMC:GG2.GP7, SC:GG2.GP4]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers	
	Goal 6 – Technology asset supply chain risks are managed.			
	1.	Does the acquirer identify and document the resilience requirements for technology assets that support the critical service? [TM:SG2.SP1]	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	
	2.	Does the acquirer evaluate technology assets that support the critical service for vulnerabilities before they are acquired? [VAR:SG2.SP2]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.RA-1:** Asset vulnerabilities are identified and documented	
	3.	Has the acquirer identified the criteria or standards required for technology suppliers to be considered trusted? [EXD:SG3.SP1]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
	4.	Has the acquirer identified trusted suppliers from which it obtains technology assets that support the critical service? [TM:SG3.SP2, TM:GG2.GP2]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
	5.	Does the acquirer formally evaluate the need to conduct acceptance testing for technology assets that support the critical service and conduct such testing (if appropriate)? [TM:SG2.SP2]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **PR.IP-2:** A System Development Life Cycle to manage systems is implemented	

	EDM Self-Assessment		NIST CSF References	Notes
	2 Relationship Management and Governance The purpose of Relationship Management and Governance is to assess whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk. This includes identifying the external entities that support the critical service, ongoing risk management, communicating with external entities about key aspects of protecting the critical service, and controlling external entities' access to the acquirer.			
	Goal 1 – External dependencies are identified and prioritized.			
	1.	Are dependencies on external entities that are critical to the service(s) identified? [EXD:SG1.SP1]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
		1.1 Suppliers		
		1.2 Infrastructure providers		
		1.3 Governmental services		
	2.	Are external dependencies prioritized? [EXD:SG1.SP2]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
	3.	Has a process been established for maintaining a list of external dependencies and related information? [EXD:SG1.SP1]	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
	Goal 2 – Supplier risk management is continuous.			
	1.	Does the acquirer periodically review and update resilience requirements for suppliers? [RRM:SG1.SP3]	**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 for all operating states (e.g. under duress/attack, during recovery, normal operations) **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	2.	Does the acquirer periodically review risks due to suppliers? [EXD:SG2.SP1]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	3.	Does the acquirer periodically discuss and review risks with suppliers? [EXD:GG2.GP7, RISK:GG2.GP8]	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	4.	Does the acquirer conduct periodic reviews with suppliers to verify that vulnerabilities relevant to the critical service are continuously managed? [VAR:GG2.GP7, VAR:GG2.GP8]	**ID.RA-1:** Asset vulnerabilities are identified and documented **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **PR.IP-12:** A vulnerability management plan is developed and implemented **DE.CM-8:** Vulnerability scans are performed **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	

	EDM Self-Assessment		NIST CSF References	Notes
	5.	Does the acquirer's risk monitoring include critical service resilience requirements not codified in supplier agreements? [RISK:SG5.SP2]	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	6.	Does the acquirer's risk monitoring include supplier performance issues and concerns? [RISK:SG5.SP2]	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	Goal 3 – Supplier performance is governed and managed.			
	1.	Does the acquirer monitor the performance of suppliers against resilience requirements? [EXD:SG4.SP1]	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events	PR.IP-5 is mapped to specific practices in the CRR that are not included in the EDM assessment due to its scope, focusing on supply chain risk management.
	2.	Are issues with supplier performance documented and reported to appropriate stakeholders? [EXD:GG2.GP7]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	3.	Does the acquirer take corrective actions as necessary to address issues with supplier performance? [EXD:SG4.SP2]	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	4.	Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	Goal 4 – Change and capacity management are applied to external dependencies.			
	1.	Does the acquirer have a change management process to manage modifications to its own assets that support the critical service? [ADM:SG3.SP2]	**PR.IP-3:** Configuration change control processes are in place	
		1.1 Information		
		1.2 Technology		
		1.3 Facilities		
		1.4 People		
	2.	Are changes to assets that support the critical service (whether located at the acquirer or at suppliers) coordinated between the acquirer and suppliers? [ADM:GG2.GP7]	**PR.IP-3:** Configuration change control processes are in place **PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	

	EDM Self-Assessment		NIST CSF References	Notes
		2.1 Information *2.2 Technology* *2.3 Facilities* *2.4 People*		
	3.	Is there a process to monitor contract renegotiations, updates, addendums, and similar changes to identify and manage any impacts to the critical service? [EXD:SG3.SP4]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	4.	Does the acquirer monitor for organizational changes at external entities - for example buy-outs, financial problems, political or civil problems - that may affect the critical service? [MON:SG1.SP1]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events	
	5.	Does the acquirer manage the capacity of services and assets cooperatively with suppliers? [TM:SG5.SP3]	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **PR.DS-4:** Adequate capacity to ensure availability is maintained	
	Goal 5 – Supplier transitions are managed.			
	1.	Has the acquirer identified criteria or conditions that would cause it to terminate supplier formal agreements? [EXD:SG4.SP2]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **PR.IP-2:** A System Development Life Cycle to manage systems is implemented	
	2.	Has the acquirer planned the actions it will take to sustain the critical service if one or more supplier formal agreements are terminated (by either the acquirer or supplier)? [EXD:GG2.GP1]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	3.	Does the acquirer use lessons learned from supplier transitions to refine its external dependencies management processes? [EXD:GG3.GP2]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **PR.IP-7:** Protection processes are improved **PR.IP-8:** Effectiveness of protection technologies is shared	
	Goal 6 – Infrastructure and governmental dependencies are managed.			
	1.	Does the acquirer have a process to periodically review and update resilience requirements for infrastructure providers that support the critical service? [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 for all operating states (e.g. under duress/attack, during recovery, normal operations) **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	

	EDM Self-Assessment		NIST CSF References	Notes
	2.	Has responsibility been assigned for monitoring the performance of infrastructure providers that support the critical service? [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.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	This EDM practice informs the NIST CSF references, although the CSF does not address the establishment of responsibility.
	3.	Has responsibility been assigned for managing relationships with the providers of governmental services that support the critical service? [EXD:SG4.SP1, EXD:GG2.SP7]	**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:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	This EDM practice informs the NIST CSF references, although the CSF does not address the establishment of responsibility.
	4.	Are performance (or other) issues involving infrastructure providers and governmental services communicated to stakeholders for use in managing the dependency? [EXD:GG2.GP7]	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	5.	Does the acquirer's risk monitoring include performance (or other) issues involving infrastructure providers and governmental services? [RISK:SG5.SP2]	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	
	Goal 7 – External entity access to acquirer assets is managed.			
	1.	Are both local and remote access to acquirer assets that support the critical service granted based on the assets' protection requirements? [AM:SG1.SP1]	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	The CRR has specific questions about remote maintenance, a topic that is not specifically covered in the EDM practices. As such, it is mapped to this EDM practice regarding remote access.
	2.	Does the acquirer have a process to appropriately modify access privileges when an external entity has personnel changes such as terminations, promotions, or job changes? [AM:SG1.SP2]	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	3.	Does the acquirer periodically review external entity access privileges - granted to external entity personnel or systems - to identify and correct inappropriate access privileges to acquirer assets? [AM:SG1.SP3]	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed	

	EDM Self-Assessment		NIST CSF References	Notes
		3.1 Information		
		3.2 Technology		
		3.3 Facilities		
	4.	Does the acquirer identify inappropriate access attempts (for example by periodically reviewing access logs) by external entity personnel or systems to acquirer assets? [IMC:SG2.SP1]	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	
		4.1 Information		
		4.2 Technology		
		4.3 Facilities		

	EDM Self-Assessment		NIST CSF References	Notes
	3 Service Protection and Sustainment The purpose of Service Protection and Sustainment is to assess whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents and threats. This includes integrating external entity considerations into the acquirer's disruption planning - typically incident management and business continuity, validating controls at external entities, and maintaining situational awareness activities directed at external dependencies.			
	Goal 1 – Disruption planning includes external dependencies.			
	1.	Does the acquirer have an incident management plan to protect the critical service? [IMC:SG1.SP1]	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	2.	Have incident declaration criteria that support the critical service been established and communicated to relevant external entities? [IMC:SG3.SP1, IMC:GG2.GP7]	**DE.AE-5:** Incident alert thresholds are established	
	3.	Does the acquirer have a documented service continuity/business continuity plan to sustain the critical service? [SC:SG3.SP2]	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	4.	Do the acquirer's plans account for dependence on external entities? [EXD:SG2.SP2, SC:SG3.SP2] *4.1 Incident management* *4.2 Service continuity*	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	5.	Do relevant external entities participate in the acquirer's planning activities? [IMC:GG2.GP7, SC:SG2.SP2] *5.1 Incident management* *5.2 Service continuity*	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers **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 – Planning and controls are maintained and updated.			
	1.	Are disruption management plans tested cooperatively with relevant suppliers? [SC:SG5.SP3, IMC:GG2.GP7] *1.1 Incident management* *1.2 Service continuity*	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers	
	2.	Do changes in external entity relationships trigger a review of disruption management plans? [IMC:GG2.GP8, SC:SG7.SP1] *2.1 Incident management* *2.2 Service continuity*	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
	3.	Are controls at suppliers that support the critical service periodically validated or tested to ensure they meet control objectives? [CTRL:SG4.SP1, EXD:SG4.SP1]	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	

	EDM Self-Assessment		NIST CSF References	Notes
	4.	Does the acquirer have a documented list of triggering events or changes that require testing of controls at suppliers that support the critical service? [CTRL:SG4.SP1, EXD:SG4.SP1]	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	Goal 3 – Situational awareness extends to external dependencies.			
	1.	Has the acquirer assigned responsibility internally for monitoring sources of threat information? [MON:SG1.SP2]	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities	This EDM practice informs the NIST CSF references, although the CSF does not address the establishment of responsibility.
	2.	Has the acquirer implemented threat monitoring procedures, including how threats are received and responded to? [MON:SG2.SP2]	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **ID.RA-3:** Threats, both internal and external, are identified and documented	
	3.	Does the acquirer identify external entities that it should include as part of its threat monitoring activities? [MON:SG1.SP3]	**ID.RA-3:** Threats, both internal and external, are identified and documented **PR.IP-8:** Effectiveness of protection technologies is shared **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
		3.1 Suppliers *3.2 Infrastructure providers*		
	4.	Do the acquirer and relevant external entities exchange information about threats to the critical service? [MON:SG2.SP2]	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **PR.IP-8:** Effectiveness of protection technologies is shared **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	5.	Does the acquirer participate in or take advantage of industry consortia (i.e., InfraGard, Coordinating Councils, Council of Supply Chain Management) to detect threats to the acquirer and external entities? [MON:SG2.SP1, MON:GG2.GP7]	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	6.	Are threats to external entities reported to internal stakeholders for use in managing the dependency? [MON:SG1.SP3, MON:SG2.SP4]	**PR.IP-8:** Effectiveness of protection technologies is shared **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	

	EDM Self-Assessment		NIST CSF References	Notes
MIL2-Planned	1.	Is there a documented plan for performing external dependencies management?		
	2.	Is there a documented policy for external dependencies management?		
	3.	Does the plan or policy identify and describe external dependencies management processes?		
	4.	Have internal and external stakeholders for external dependencies management activities been identified and made aware of their cybersecurity roles?		
	5.	Have external dependencies management standards, guidelines and roles been established and implemented?		
MIL3-Managed	1.	Is there management oversight of the performance of external dependencies management?		
	2.	Are the acquirer's external dependencies management processes periodically reviewed to identify and manage risks to these processes?		
	3.	Have qualified staff been assigned to perform external dependencies management activities as planned?		
	4.	Is there adequate funding to perform external dependencies management activities as planned?		
MIL4-Measured	1.	Are external dependencies management activities measured and periodically reviewed to ensure they are effective and producing intended results?		
	2.	Are external dependencies management activities periodically reviewed to ensure they are adhering to the plan?		
	3.	Is *higher level* management aware of issues related to the performance of external dependencies management?		
MIL5-Defined	1.	Has the acquirer identified, described, and disseminated standard external dependencies management processes that apply across the enterprise?		
	2.	Has the acquirer provided individual operating units with guidelines to help them tailor standard enterprise processes to fit their unique operating circumstances?		
	3.	Are improvements to external dependencies management documented and shared across the acquirer enterprise?		

Crosswalk Reference Key

External Dependencies Management Assessment (EDM) Reference Key	
F	Facilities
G	Governmental Services
G*x*	Goal
I	Information
IM	Incident Management
IP	Infrastructure Providers
MIL	Maturity Indicator Level
P	People
Q*x*	Question
RF	Relationship Formation
RMG	Relationship Management and Governance
S	Supplier
SC	Service Continuity
SPS	Service Protection and Sustainment
T	Technology

CERT® Resilience Management Model (CERT®-RMM) Reference Key*	
ADM	Asset Definition and Management
AM	Access Management
CTRL	Controls Management
EF	Enterprise Focus
EXD	External Dependencies Management
GG*x*	Generic Goal
IMC	Incident Management and Control
MON	Monitoring
RISK	Risk Management
RRM	Resilience Requirements Management
SC	Service Continuity
SG*x*	Specific Goal
SP*x*	Specific Practice
TM	Technology Management
VAR	Vulnerability Awareness and Resolution

References	
CRR	http://www.us-cert.gov/ccubedvp/self-service-crr
RMM	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

* RMM references for the EDM questions can be found in the EDM to CSF Crosswalk starting on page 15.

This page is intentionally blank.

Homeland
Security