INSIDER RISK MANAGEMENT PROGRAM EVALUATION (IRMPE)

NIST Cybersecurity Framework and Other Standards Crosswalk

SEPTEMBER 2021

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

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM21-0340

Contents

Notification

This document is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this document, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the document.

DHS does not endorse any commercial product or service, including the subject of the analysis referred to in this document. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this document shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

NIST Cybersecurity Framework (CSF) to Insider Risk Self-Assessment Crosswalk

Identify (ID)

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
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	PM:G5:Q4		• 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	PM:G5: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		• 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	PM:G5:Q5		• 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	PM:G5:Q1 PM:G5: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	PM:G5:Q6 PT:G1:Q1	PM:MIL2 PM:MIL3	• 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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	N/A		• 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		• 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	PM:G1:Q1		• 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	PM:G5:Q1 PM:G5:Q3 PM:G5:Q5		• 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)	N/A		• 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

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
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	PM:G1:Q1 PM:G1:Q2 PM:G3:Q1 CA:G5:Q1	PM:MIL2 PM:MIL3 CA:MIL5 PT:MIL5	• 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	PM:G1:Q1 PM:G5:Q6 PT:G2:Q1 PT:G2:Q2	PM:MIL2 PT:MIL2	• 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	PM:G1:Q2 CA:G2:Q7	PM:MIL2 CA:MIL3	• 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	PM:G4:Q4 CA:G5:Q1	PT:MIL3	• 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	N/A		• 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	CA:G2:Q6		• 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	PM:G2:Q1 PM:G4:Q1 PM:G4:Q2 PM:G4:Q4 PM:G4:Q5 CA:G5:Q1		• 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	PM:G4: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	PM:G4: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
		ID.RA-6: Risk responses are identified and prioritized	PM:G4:Q3		• 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 •

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
Identify (ID)	**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	PM:G4:Q3 PM:G4:Q4 PM:G4:Q5	PM:MIL3	• 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		• 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		• 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	PM:G5:Q5		• 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	N/A		• 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.	N/A		• 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.	N/A		• 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
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	N/A		• 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)

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
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	PM:G2:Q4	• 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	N/A	• 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	N/A	• 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	PM:G2:Q4	• 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	• 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	PM:G2:Q4	• 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
		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)	PM:G2:Q4	• 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

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
Protect (PR)	**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	PT:G4:Q1 PT:G5:Q1		• 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	PT:G3:Q1 PT:G6:Q1		• 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	N/A		• 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	PT:G7:Q1	PT:MIL4	• 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	PT:G2:Q3 PT:G3:Q1 PT:G6:Q3		• 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	CA:G2:Q2		• 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	CA:G2:Q2		• 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	CA:G2:Q2		• 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
		PR.DS-4: Adequate capacity to ensure availability is maintained	CA:G2:Q3		• 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	CA:G2:Q2		• 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

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
Protect (PR)	**Data Security (DS), continued:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	CA:G2:Q2	• 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	• 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	• 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	• 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	N/A	• 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	N/A	• 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	• 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
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	N/A	• 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	• 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	N/A	• 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

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
Protect (PR)	**Information Protection Processes and Procedures (IP) continued:** 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-8:** Effectiveness of protection technologies is shared	N/A	• 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	CA:G1:Q8	• 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		• 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)	CA:G2:Q5 CA:G6:Q1 CA:G6:Q2 CA:G7:Q1 CA:G7:Q2 CA:G7:Q3 CA:G7:Q4 CA:G8:Q1 PM:G2:Q3	• 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	N/A	• 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	N/A	• 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	N/A	• 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
	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	PM:G2:Q3	• 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 •

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
Protect (PR)	**Protective Technology (PT) continued:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-2:** Removable media is protected and its use restricted according to policy	PM:G2:Q3	• 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	PM:G2:Q3	• 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	PM:G2:Q3	• 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	PM:G2:Q3	• 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)

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
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	CA:G5:Q3	• 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	CA:G1:Q2	• 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

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
Detect (DE)	**Anomalies and Events (AE) continued:** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors	CA:G2:Q1 CA:G2:Q4 CA:G2:Q5 CA:G3:Q2 CA:G3:Q3 CA:G4:Q1 CA:G5:Q3 CA:G8:Q1 PM:G2:Q2 PM:G2:Q3	• 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
		DE.AE-4: Impact of events is determined	CA:G1:Q8	• 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	CA:G8:Q1	• 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	CA:G3:Q2 CA:G4:Q1 PM:G2:Q2 PM:G2:Q4	• 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	CA:G2:Q5 PM:G2:Q2 PM:G2:Q4	• 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	CA:G2:Q5 CA:G4:Q1 CA:G5:Q3 CA:G7:Q1 CA:G7:Q2 CA:G8:Q1 PM:G2:Q2 PM:G2:Q4	• 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	• 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	• 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	N/A	• 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

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
Detect (DE)	**Security Continuous Monitoring (CM) continued:** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	CA:G3:Q2		• 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	N/A		• 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	CA:G1:Q4 CA:G1:Q5 CA:G5:Q2	CA:MIL2	• 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
		DE.DP-2: Detection activities comply with all applicable requirements	CA:G3:Q1 CA:G8:Q1	CA:MIL2	• 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	CA:MIL4	• 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	CA:G1:Q5 CA:G2:Q1 CA:G2:Q5 PM:G2:Q2		• 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	CA:G2:Q8 CA:G2:Q9	CA:MIL4	• 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)

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
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	CA:G1:Q2	• 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	CA:G1:Q2 CA:G1:Q4 CA:G1:Q5	• 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	PM:G3:Q2 PM:G3:Q4	• 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	PM:G3:Q3 PM:G3:Q5	• 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	PM:G3:Q3 CA:G1:Q5	• 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	PM:G3:Q4 PM: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
	Analysis (AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	CA:G4:Q1 CA:G5:Q2 CA:G5:Q3 PM:G2:Q2	• 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	• 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	CA:G1:Q6 CA:G1:Q7	• 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

Function	Category	Subcategory	IRPME Reference(s)	Informative References for NIST CSF
Respond (RS)	**Analysis (AN) continued:** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-4:** Incidents are categorized consistent with response plans	PM:G2:Q2	• 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)	CA:G2:Q6	• 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	CA:G1:Q1 PM:G2:Q2	• 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	CA:G1:Q1 PM:G2:Q2	• 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	N/A	• 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	• 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	• 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

Recover (RC)

Function	Category	Subcategory	IRPME Reference(s)		Informative References for NIST CSF
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	CA:G1:Q8		• 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		• 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		• 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		• 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		• 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	CA:MIL5	• COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4

Insider Risk Self-Assessment to Cybersecurity Frameworks Crosswalk

Program Management

The purpose of the Program Management domain is to determine whether the organization has the management structures, policies, relationships, and communications in place needed as a foundation for an Insider Risk Program. Program Management includes

(1) understanding mission critical assets,
(2) defining the Insider Risk policy for the organization,
(3) characterizing the activities associated with insider threat prevention, detection and response,
(4) ensuring communication of insider threat activities and events among responsible participants in the Insider Risk program,
(5) providing governance and oversite of insider risk activities, and
(6) integrating insider risk management with organizational or enterprise risk management generally.

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 1 - An Insider Risk policy exists.			
1. Is there an authoritative document that establishes the existence of the Insider Risk program?	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated **ID.GV-1:** Organizational cybersecurity policy is established and communicated **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2. Does the authoritative document define the program's: • authority • scope • roles and responsibilities for stakeholders	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 2 - There is detect, identify, assess, and manage capability for insider threat events.			
1. Are the types of insider threats to be addressed identified and documented?	**ID.RA-3:** Threats, both internal and external, are identified and documented	(1) Know and protect your critical assets.	• NIST SP 800-53 Rev. 5 AC-3, AU-12, CA-7, CM-11, CM-12, CM-13, CM-2, CM-7, CM-8, CP-2, IR-3, IR-8, PE-23, PE-3, PL-10, PL-11, PM-17, PM-18, PM-19, PM-22,PM-29, PM-5, PM-8, PT-2, PT-3, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-17, SA-23, SA-3, SA-4, SA-8, SC-47, SC-7, SC-8, SI-19, SI-23, SI-4, SR-4 • National Insider Threat Policy B-2 • Minimum Standards G-1-b, G-1-c • CERT-RMM Asset Definition and Management, Enterprise Focus • CIS CSC 1, 2 • CMMC AM.4.226, CM.2.061, CM.2.064

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
2.	Has a capability been established that supports detection, investigation, and response to insider threat types identified?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **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 **RS.AN-1:** Notifications from detection systems are investigated **RS.AN-4:** Incidents are categorized consistent with response plans **RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated	(3) Clearly document and consistently enforce policies and controls. (4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (12) Deploy solutions for monitoring employee actions and correlating information from multiple data sources. (13) Monitor and control remote access from all end points, including mobile devices.	• NIST SP 800-53 Rev. 5 AC-2, AC-3, AC-4, AC-12, AC-17, AC-19, AC-20, AU-1, AU-2, AU-6, AU-7, AU-12, CA-3, CA-7, CM-3, CM-11, CM-12, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-21, PM-22, PM-27, PM-29, PM-31, PS-1, PS-2, PS-3, PS-8, PS-9, PT-1, PT-2, PT-3, PT-6, RA-3, SA-8, SA-10, SA-17, SC-7, SC-8, SC-48, SI-4, SR-1 • National Insider Threat Policy C-1-1, C-1-2, C-1-4 • Minimum Standards E-1, H, H-1 • CERT-RMM Compliance, Human Resources, Monitoring, Technology Management • CIS CSC 6 • CMMC AC.1.001, AC.1.002, AC.2.013, AC.2.015, AC.3.014, AC.3.020, AC.3.021, AC.3.022, AU.2.041, AU.2.042, AU.3.045, AU.3.052, AU.5.055, CA.4.163, IR.2.097, IR.5.106, PS.2.127
3.	Has a capability been established that supports prevention/deterrence of insider threat types identified?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-2:** Removable media is protected and its use restricted according to policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **PR.PT-4:** Communications and control networks are protected **PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls. (12) Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	• NIST SP 800-53 Rev. 5 AC-4, AC-12, AC-20, AC-3, AT-2, AU-1, AU-2, AU-6, AU-7, AU-12, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-21, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-3, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B, C-1-1, C-1-2, C-1-4 • Minimum Standards G-1, H-1 • CERT-RMM Compliance, Incident Management and Control, Monitoring, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.2.042, AU.3.045, AU.3.052, AU.4.053, AU.5.055, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.2.097, IR.5.106, IR.5.102, SA.4.173, SI.2.216, SI.2.217
4.	Does the prevention/deterrence capability consider negative deterrence to force or constrain employees to act in the interests of the organization?	**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 **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **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)	(10) Implement strict password and account management policies and practices. (11) Institute stringent access controls and monitoring policies on privileged users.	• NIST SP 800-53 Rev. 5 AC-2, AC-3, AC-4, AC-6, AC-7, AC-17, AC-20, AU-2, AU-3, AU-5, AU-6, AU-9, CA-3, CA-6, CM-3, CM-5, CM-7, CM-11, CM-12, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, MA-7, PE-3, PL-4, PM-21, PM-31, PS-3, PT-2, PT-3, SA-5, SA-8, SA-9, SC-45, SC-48, SI-10, SR-3, SR-4, SR-5 • National Insider Threat Policy B-7, C-1-1, C-1-7 • Minimum Standards G-1-b, H-1 • CERT-RMM Identify/Access Management, Monitoring • CIS CSC 4, 16 • CMMC AC.1.001, AC.1.002, AC.2.013, AC.2.015, AC.3.014, AC.3.021, AU.2.041, AU.2.042, AU.3.045, AU.3.049, AU.3.050, CM.3.067, IA.1.076, IA.1.077, IA.3.083, IA.3.084, IR.2.097, MA.2.114
5.	Does the prevention/deterrence capability consider positive deterrence to attract employees to act in the interests of the organization, including the timely and generally supportive resolution of employee grievances?	N/A	(21) Adopt positive incentives to align workforce with the organization.	• CERT-RMM Human Resources
6.	Are employee assistance programs available to help employees with personal and professional stressors that could motivate insider threats or incidents?	N/A	(5) Anticipate and manage negative issues in the work environment. (21) Adopt positive incentives to align workforce with the organization.	• NIST SP 800-53 Rev. 5 AC-20, PL-4, PS-1, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-2 • Minimum Standards E • CERT-RMM Human Resources

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 3 - Communication about insider threat events happens.				
1.	Is there a policy or practice in place that defines what parts of the insider risk program / capability are publicly communicated to organizational staff?	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Are there thresholds for when internal teams or groups need to be informed of an insider threat or incident?	**RS.CO-2:** Incidents are reported consistent with established criteria	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
3.	Is there a defined process in place for internal information sharing about an insider threat or incident?	**RS.CO-3:** Information is shared consistent with response plans **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
4.	Are there thresholds for when external groups (e.g., law enforcement, legal counsel, or the public) need to be informed of an insider threat or incident?	**RC.CO-1:** Public relations are managed **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217 •

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
5.	Is there a defined process in place for external information sharing about an insider threat or incident when escalation thresholds require it?	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed **RS.CO-2:** Incidents are reported consistent with established criteria **RS.CO-3:** Information is shared consistent with response plans **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 4 - Insider risk is integrated with the enterprise risk program (ERP) and/or security risk management program.				
1.	Are there procedures for conducting trusted insider risk assessments?	**ID.RA-3:** Threats, both internal and external, are identified and documented	(6) Consider threats from insiders and business partners in enterprise-wide risk assessments.	• NIST SP 800-53 Rev. 5 AT-2, AU-3, CM-13, PE-22, PE-23, PE-8, PL-10, PL-11, PM-18, PM-28, PM-30, PM-31, PM-9, PT-2, PT-3, PT-5, RA-1, RA-10, RA-3, RA-7, RA-8, SA-3, SA-4, SA-8, SC-12, SI-12, SR-1, SR-12, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7 • National Insider Threat Policy B-2, C-6 • Minimum Standards E-1, G, J • CERT-RMM Access Control and Management, External Dependencies Management, Human Resources Management • CMMC RM.2.141
2.	Is a trusted insider risk assessment done on a yearly basis, and are the results integrated with the organization's Enterprise Risk Program (ERP) or security risk program?	**ID.RA-3:** Threats, both internal and external, are identified and documented	(6) Consider threats from insiders and business partners in enterprise-wide risk assessments.	• NIST SP 800-53 Rev. 5 AT-2, AU-3, CM-13, PE-22, PE-23, PE-8, PL-10, PL-11, PM-18, PM-28, PM-30, PM-31, PM-9, PT-2, PT-3, PT-5, RA-1, RA-10, RA-3, RA-7, RA-8, SA-3, SA-4, SA-8, SC-12, SI-12, SR-1, SR-12, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7 • National Insider Threat Policy B-2, C-6 • Minimum Standards E-1, G, J • CERT-RMM Access Control and Management, External Dependencies Management, Human Resources Management • CMMC RM.2.141
3.	Have criteria been defined for trusted insider risks (probability, impact, priority, tolerance) that are consistent with ERP risk criteria?	**ID.RA-4:** Potential business impacts and likelihoods are identified **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **ID.RA-6:** Risk responses are identified and prioritized	(6) Consider threats from insiders and business partners in enterprise-wide risk assessments.	• NIST SP 800-53 Rev. 5 AT-2, AU-3, CM-13, PE-22, PE-23, PE-8, PL-10, PL-11, PM-18, PM-28, PM-30, PM-31, PM-9, PT-2, PT-3, PT-5, RA-1, RA-10, RA-3, RA-7, RA-8, SA-3, SA-4, SA-8, SC-12, SI-12, SR-1, SR-12, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7 • National Insider Threat Policy B-2, C-6 • Minimum Standards E-1, G, J • CERT-RMM Access Control and Management, External Dependencies Management, Human Resources Management • CMMC RM.2.141
4.	Are trusted Insider risks treated as a category of risk in the ERP?	**ID.RA-3:** Threats, both internal and external, are identified and documented	(6) Consider threats from insiders and business partners in enterprise-wide risk assessments.	• NIST SP 800-53 Rev. 5 AT-2, AU-3, CM-13, PE-22, PE-23, PE-8, PL-10, PL-11, PM-18, PM-28, PM-30, PM-31, PM-9, PT-2, PT-3, PT-5, RA-1, RA-10, RA-3, RA-7, RA-8, SA-3, SA-4, SA-8, SC-12, SI-12, SR-1, SR-12, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7 • National Insider Threat Policy B-2, C-6 • Minimum Standards E-1, G, J • CERT-RMM Access Control and Management, External Dependencies Management, Human Resources Management • CMMC RM.2.141
5.	Are trusted insider risks identified and integrated into the ERP on a continuous basis?	**ID.RA-3:** Threats, both internal and external, are identified and documented	(6) Consider threats from insiders and business partners in enterprise-wide risk assessments.	• NIST SP 800-53 Rev. 5 AT-2, AU-3, CM-13, PE-22, PE-23, PE-8, PL-10, PL-11, PM-18, PM-28, PM-30, PM-31, PM-9, PT-2, PT-3, PT-5, RA-1, RA-10, RA-3, RA-7, RA-8, SA-3, SA-4, SA-8, SC-12, SI-12, SR-1, SR-12, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7 • National Insider Threat Policy B-2, C-6 • Minimum Standards E-1, G, J • CERT-RMM Access Control and Management, External Dependencies Management, Human Resources Management • CMMC RM.2.141

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 5 - Mission-critical assets are known.				
1.	Is an inventory of critical assets maintained to support the Insider Risk program?	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	(1) Know and protect your critical assets.	• NIST SP 800-53 Rev. 5 AC-3, AU-12, CA-7, CM-11, CM-12, CM-13, CM-2, CM-7, CM-8, CP-2, IR-3, IR-8, PE-23, PE-3, PL-10, PL-11, PM-17, PM-18, PM-19, PM-22,PM-29, PM-5, PM-8, PT-2, PT-3, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-17, SA-23, SA-3, SA-4, SA-8, SC-47, SC-7, SC-8, SI-19, SI-23, SI-4, SR-4 • National Insider Threat Policy B-2 • Minimum Standards G-1-b, G-1-c • CERT-RMM Asset Definition and Management, Enterprise Focus • CIS CSC 1, 2 • CMMC AM.4.226, CM.2.061, CM.2.064
2.	Are critical assets associated with key or primary users who may pose particular insider risk?	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	(1) Know and protect your critical assets. (11) Institute stringent access controls and monitoring policies on privileged users.	• NIST SP 800-53 Rev. 5 AC-2, AC-17, AC-20, AC-3, AC-4, AC-6, AU-2, AU-3, AU-5, AU-6, AU-9, AU-12, CA-6, CA-7, CM-11, CM-12, CM-13, CM-2, CM-3, CM-5, CM-7, CM-8, CP-2, IA-2, IA-12, IR-3, IR-8, MA-3, MA-5, MA-7, PE-3, PE-23, PL-10, PL-11, PL-4, PM-17, PM-18, PM-19, PM-21, PM-22, PM-29, PM-31, PM-5, PM-8, PS-3, PT-2, PT-3, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-3, SA-4, SA-5, SA-8, SA-9, SA-17, SA-23, SC-7, SC-8, SC-45, SC-47, SC-48, SI-4, SI-10, SI-19, SI-23, SR-3, SR-4, SR-5 • National Insider Threat Policy B-2, C-1-1 • Minimum Standards G-1-b, H-1 • CERT-RMM Asset Definition and Management, Enterprise Focus, Identity/Access Management, Monitoring • CIS CSC 1, 2, 4 • CMMC AC.1.001, AC.1.002, AC.2.013, AC.2.015, AC.3.014, AC.3.021, AM.4.226, AU.2.041, AU.2.042, AU.3.045, AU.3.049, AU.3.050, CM.2.061, CM.2.064, CM.3.067, IA.1.076, IA.1.077, IA.3.083, IA.3.084, IR.2.097, MA.2.114
3.	Have critical software platforms and applications within the organization been identified in support of detection, investigation, and response to insider threats?	**ID.AM-2:** Software platforms and applications within the organization are inventoried	(12) Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	• NIST SP 800-53 Rev. 5 AC-4, AU-1, AU-12, AU-2, AU-6, AU-7, CM-3, IR-3, IR-4, IR-8, PM-21, PM-31, RA-3, SA-8, SC-48 • National Insider Threat Policy C-1-1, C-1-2, C-1-4 • Minimum Standards H-1 • CERT-RMM Monitoring • CIS CSC 6 • CMMC AU.2.041, AU.2.042, AU.3.045, AU.3.052, AU.5.055, IR.2.097, IR.5.106
4.	Have critical physical IT assets been identified in support of detection, investigation, and response for insider threats?	**ID.AM-1:** Physical devices and systems within the organization are inventoried	(1) Know and protect your critical assets.	• NIST SP 800-53 Rev. 5 AC-3, AU-12, CA-7, CM-11, CM-12, CM-13, CM-2, CM-7, CM-8, CP-2, IR-3, IR-8, PE-23, PE-3, PL-10, PL-11, PM-17, PM-18, PM-19, PM-22,PM-29, PM-5, PM-8, PT-2, PT-3, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-17, SA-23, SA-3, SA-4, SA-8, SC-47, SC-7, SC-8, SI-19, SI-23, SI-4, SR-4 • National Insider Threat Policy B-2 • Minimum Standards G-1-b, G-1-c • CERT-RMM Asset Definition and Management, Enterprise Focus • CIS CSC 1, 2 • CMMC AM.4.226, CM.2.061, CM.2.064 •

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
5.	Are critical services associated with third parties that may represent insider risk?	**ID.AM-4:** External information systems are catalogued	(1) Know and protect your critical assets. (6) Consider threats from insiders and business partners in enterprise-wide risk assessments. (16) Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	• NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-13, AC-14, AC-15, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-23, AC-24, AC-25, AT-2, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16, CA-3, CA-6, CA-7, CM-2, CM-3, CM-7, CM-8, CM-11, CM-12, CM-13, CM-14, CP-2, CP-9, IA-5, IA-12, IR-3, IR-8, MA-3, PE-3, PE-8, PE-22, PE-23, PL-10, PL-11, PM-5, PM-7, PM-8, PM-9, PM-17, PM-18, PM-19, PM-20, PM-21, PM-22, PM-24, PM-25, PM-28, PM-29, PM-30, PM-31, PM-32, PT-2, PT-3, PT-4, PT-5, PT-6, PT-7, RA-1, RA-1, RA-10, RA-2, RA-3, RA-4, RA-5, RA-6, RA-7, RA-8, RA-9, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-10, SA-11, SA-12, SA-13, SA-14, SA-15, SA-16, SA-17, SA-18, SA-19, SA-20, SA-21, SA-22, SA-23, SC-1, SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-15, SC-16, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-26, SC-27, SC-28, SC-42, SC-45, SC-46, SC-47, SC-48, SC-49, SC-50, SI-4, SI-10, SI-12, SI-14, SI-18, SI-19, SI-20, SI-23, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-9, SR-11, SR-12 • National Insider Threat Policy B-2, C-6 • Minimum Stanadrds E-1, G, G-1-b, G-1-c, H-1, J • CERT-RMM Asset Control and Management, Asset Definition and Management, Enterprise Focus, External Dependencies Management, Human Resources Management • CIS CSC 1, 2 • CMMC AM.4.226, CM.2.061, CM.2.064, RM.2.141
6.	Are cybersecurity roles and responsibilities established to define organizational accountability for addressing insider risk?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Maturity Indicator Level (MIL) 2 - Planned				
1.	Is there a plan for performing program management activities?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-1:** Organizational cybersecurity policy is established and communicated	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Is there a documented policy for program management?			
3.	Have stakeholders for program management activities been identified and made aware of their roles?			
4.	Have program management standards and guidelines been identified and implemented?			
Maturity Indicator Level (MIL) 3 – Managed				
1.	Is there oversight of the Insider Risk program?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.GV-1:** Organizational cybersecurity policy is established and communicated	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Have qualified staff been assigned to perform program management activities?			
3.	Is there adequate funding to perform program management activities as planned?			
4.	Are risks related to the performance of planned program management activities identified, analyzed, disposed of, monitored, and controlled?			

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Maturity Indicator Level (MIL) 4 - Measured			
1. Are program management activities periodically reviewed and measured to ensure they are effective and producing intended results? 2. Are program 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 program management?	N/A	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Maturity Indicator Level (MIL) 5 - Defined			
1. Has the organization adopted a standard definition of program management activities from which operating units can derive practices that fit their unique operating circumstances? 2. Are improvements to program management documented and shared across the organization?	N/A	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

Personnel and Training

The purpose of the Personnel and Training domain is to determine if the organization has instituted the appropriate levels of insider risk awareness and training throughout the employee lifecycle. Personnel and Training includes

(1) insider risk awareness training for all personnel,
(2) role-based training for employees working with the Insider Risk team,
(3) role-based training for Insider Risk program team members, and
(4) incorporation of insider risk training in the onboarding process.

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 1 - Participation in the Insider Risk Program is organization-wide.			
1. Is there cooperation from components, divisions, or departments across the organization with the Insider Risk program?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **ID.GV-4:** Governance and risk management processes address cybersecurity risks	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 2 - The Insider Risk Mitigation Team is composed of multi-disciplinary members with the appropriate skills and abilities.			
1. Are the work and tasks to be done by the Insider Risk Mitigation Team identified for all roles so that the organization can effectively build a set of required qualifications (knowledge and skills) of Insider Risk Mitigation Team members?	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2. Are Insider Risk Mitigation Team member qualifications -- such as required knowledge, skills, competencies, education, certifications, and experience – identified based on the noted tasks to be done?	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217 •

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
3.	Are Insider Risk Mitigation Team members assessed on their knowledge and skills (or competencies) and any other identified qualifications?	**PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 3 - The Insider Risk Mitigation Team receives training to enable them to handle their roles and tasks.				
1.	Is training identified and provided to Insider Risk Mitigation Team members to enable them to effectively carry out their roles and tasks?	**PR.AT-2:** Privileged users understand their roles and responsibilities **PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Is the identification and completion of Insider Risk Mitigation Team member training tracked?	N/A	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 4 - Insider risk awareness training is provided for all organizational personnel.				
1.	Is insider risk awareness training provided for all organizational personnel?	**PR.AT-1:** All users are informed and trained	(9) Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	• NIST SP 800-53 Rev. 5 AT-1, AT-2, AT-3, AT-7, IR-2, IR-4, PM-23, PT-2, PT-3, RA-3, SA-8, SR-10, SR-11, SR-4, SR-5 • National Insider Threat Policy C-1-3 • Minimum Standards I • CIS CSC 17 • CMMC AT.2.056, AT.2.057
Goal 5 - New employees are made aware of the Insider Risk Mitigation Team during the onboarding process.				
1.	Does the onboarding process for new employees inform the employee of the Insider Risk Program Team and provide guidance for how the employees should interact with that team?	**PR.AT-1:** All users are informed and trained	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 6 - Role-based insider threat awareness training is provided to staff (HR, Security, IT, Legal, Contracts, Finance, etc.) regarding detection, identification, assessment, and management of insider threat behaviors and events.			
1. Are roles that require role-based insider risk training identified?	**PR.AT-2:** Privileged users understand their roles and responsibilities	(1) Know and protect your critical assets. (2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AC-3, AT-2, AU-12, AU-6, CA-7, CM-11, CM-12, CM-13, CM-2, CM-3, CM-7, CM-8, CP-2, IR-2, IR-3, IR-4, IR-8, PE-23, PE-3, PL-10, PL-11, PM-17, PM-18, PM-19, PM-22, PM-23, PM-29, PM-31, PM-5, PM-8, PT-2, PT-3, PT-7, RA-10, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-17, SA-23, SA-3, SA-4, SA-8, SC-16, SC-47, SC-48, SC-7, SC-8, SI-18, SI-19, SI-23, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B, B-2 • Minimum Standards G-1, G-1-b, G-1-c • CERT-RMM Asset Definition and Management, Enterprise Focus, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 1, 2, 3 • CMMC AC.5.024, AM.4.226, AT.2.056, AU.2.041, AU.4.053, CM.2.061, CM.2.064, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2. Are staff / resources assigned to manage, coordinate, and support role-based insider risk training?	N/A	(1) Know and protect your critical assets. (2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AC-3, AT-2, AU-12, AU-6, CA-7, CM-11, CM-12, CM-13, CM-2, CM-3, CM-7, CM-8, CP-2, IR-2, IR-3, IR-4, IR-8, PE-23, PE-3, PL-10, PL-11, PM-17, PM-18, PM-19, PM-22, PM-23, PM-29, PM-31, PM-5, PM-8, PT-2, PT-3, PT-7, RA-10, RA-2, RA-3, RA-7, RA-8, RA-9, SA-10, SA-17, SA-23, SA-3, SA-4, SA-8, SC-16, SC-47, SC-48, SC-7, SC-8, SI-18, SI-19, SI-23, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B, B-2 • Minimum Standards G-1, G-1-b, G-1-c • CERT-RMM Asset Definition and Management, Enterprise Focus, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 1, 2, 3 • CMMC AC.5.024, AM.4.226, AT.2.056, AU.2.041, AU.4.053, CM.2.061, CM.2.064, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
3. Is role-based insider risk awareness training provided to staff (HR, Security, IT, Legal, Contracts, Finance, etc.) regarding detection, identification, assessment, and management of insider risk behaviors and events?	**PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 7 - Managers and supervisors receive training regarding prevention, detection, and response to insider risk behaviors and events.			
1. Do managers and supervisors receive training regarding detection, identification, assessment, and management of insider risk behaviors and events?	**PR.AT-4:** Senior executives understand their roles and responsibilities	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (21) Adopt positive incentives to align workforce with organization.	• NIST SP 800-53 Rev. 5 AU-12 PS-1, PS-2, PS-3, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Maturity Indicator Level (MIL) 2 - Planned			
1. Is there a plan for performing personnel and training activities? 2. Is there a documented policy for personnel and training activities? 3. Have stakeholders for personnel and training activities been identified and made aware of their roles? 4. Have personnel and training standards and guidelines been identified and implemented?	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls. (9) Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	• NIST SP 800-53 Rev. 5 AC-3, AC-12, AC-20, AT-1, AT-2, AT-3, AT-7, AU-6, CA-7, CM-3, CM-11, CM-12, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-2, PT-3, PT-6, PT-7, RA-3, RA-10, SA-8, SA-10, SA-17, SC-7, SC-8, SC-16, SC-48, SI-4, SI-18, SR-1, SR-10, SR-11, SR-2, SR-4, SR-5, SR-6, SR-8, SR-9 • National Insider Threat Policy B, C-1-3 • Minimum Standards G-1, I • CERT-RMM Compliance, Incident Management and Control, Organizational Training and Awareness, Vulnerability Analysis and Resolution • CIS CSC 3, 6, 17 • CMMC AC.5.024, AT.2.056, AT.2.057, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Maturity Indicator Level (MIL) 3 - Managed			
Is there oversight of personnel and training activities? Have qualified staff been assigned to perform personnel and training activities? Is there adequate funding to perform personnel and training activities as planned? Are risks related to the performance of personnel and training activities identified, analyzed, disposed of, monitored, and controlled?	**ID.GV-4:** Governance and risk management processes address cybersecurity risks	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls. (9) Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	• NIST SP 800-53 Rev. 5 AC-3, AC-12, AC-20, AT-1, AT-2, AT-3, AT-7, AU-6, CA-7, CM-3, CM-11, CM-12, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-2, PT-3, PT-6, PT-7, RA-3, RA-10, SA-8, SA-10, SA-17, SC-7, SC-8, SC-16, SC-48, SI-4, SI-18, SR-1, SR-10, SR-11, SR-2, SR-4, SR-5, SR-6, SR-8, SR-9 • National Insider Threat Policy B, C-1-3 • Minimum Standards G-1, I • CERT-RMM Compliance, Incident Management and Control, Organizational Training and Awareness, Vulnerability Analysis and Resolution • CIS CSC 3, 6, 17 • CMMC AC.5.024, AT.2.056, AT.2.057, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Maturity Indicator Level (MIL) 4 – Measured			
1. Are personnel and training activities periodically reviewed and measured to ensure they are effective and producing intended results? 2. Are personnel and training activities periodically reviewed to ensure they are adhering to the plan? 3. Is higher-level management aware of issues related to the performance of personnel and training activities?	**PR.AT-4:** Senior executives understand their roles and responsibilities	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls. (9) Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	• NIST SP 800-53 Rev. 5 AC-3, AC-12, AC-20, AT-1, AT-2, AT-3, AT-7, AU-6, CA-7, CM-3, CM-11, CM-12, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-2, PT-3, PT-6, PT-7, RA-3, RA-10, SA-8, SA-10, SA-17, SC-7, SC-8, SC-16, SC-48, SI-4, SI-18, SR-1, SR-10, SR-11, SR-2, SR-4, SR-5, SR-6, SR-8, SR-9 • National Insider Threat Policy B, C-1-3 • Minimum Standards G-1, I • CERT-RMM Compliance, Incident Management and Control, Organizational Training and Awareness, Vulnerability Analysis and Resolution • CIS CSC 3, 6, 17 • CMMC AC.5.024, AT.2.056, AT.2.057, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Maturity Indicator Level (MIL) 5 – Defined			
1. Has the organization adopted a standard definition for personnel and training activities from which operating units can derive practices that fit their unique operating circumstances? 2. Are improvements to personnel standards and training content documented and shared across the organization?	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls. (9) Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	• NIST SP 800-53 Rev. 5 AC-3, AC-12, AC-20, AT-1, AT-2, AT-3, AT-7, AU-6, CA-7, CM-3, CM-11, CM-12, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-2, PT-3, PT-6, PT-7, RA-3, RA-10, SA-8, SA-10, SA-17, SC-7, SC-8, SC-16, SC-48, SI-4, SI-18, SR-1, SR-10, SR-11, SR-2, SR-4, SR-5, SR-6, SR-8, SR-9 • National Insider Threat Policy B, C-1-3 • Minimum Standards G-1, I • CERT-RMM Compliance, Incident Management and Control, Organizational Training and Awareness, Vulnerability Analysis and Resolution • CIS CSC 3, 6, 17 • CMMC AC.5.024, AT.2.056, AT.2.057, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

Data Collection and Analysis

The purpose of the Data Collection and Analysis domain is to identify the elements and processes necessary for the purpose of providing timely, accurate, complete, relevant, and actionable information about and response to an organization's insider risk environment. Key elements and processes include incident reporting, forensics and behavioral analytics, response mechanisms, time-focused actions, staff augmentation and organizational support, and other elements and procedures required to support an effective Insider Risk Program. The aim of all of the above is alignment with an organization's standards and policy, and compliance with relevant law and regulation.

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 1 - The organization responds to and mitigates identified potential or ongoing insider threats and incidents.				
1.	Are Identified insider threat and incidents mitigated and resolved?	**RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
2.	Does the organization follow established procedures or guidelines for responding to and mitigating insider threats and incidents?	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods **RS.RP-1:** Response plan is executed during or after an incident **RS.CO-1:** Personnel know their roles and order of operations when a response is needed	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
3.	Does resolution of insider risk matters occur in a timely fashion, as defined by organizational or federal criteria?	N/A	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
4.	Are additional staff identified and called in if needed to assist with resolving and remediating insider threat events?	**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	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
5.	Is the established chain-of-command followed to effect a disposition of all insider threat cases?	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **DE.DP-4:** Event detection information is communicated **RS.CO-1:** Personnel know their roles and order of operations when a response is needed **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
6.	Is forensic evidence collected, if necessary?	**RS.AN-3:** Forensics are performed	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
7.	Is digital media analyzed, if necessary?	**RS.AN-3:** Forensics are performed	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
8.	Do documented procedures specify the process and mechanisms to reconstitute and recover critical systems that are affected by insider risk events?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **DE.AE-4:** Impact of events is determined **RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior. (5) Anticipate and manage negative issues in the work environment.	• NIST SP 800-53 Rev. 5 AC-20, AU-12, PL-4, PS-1, PS-2, PS-3, PS-6, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards E, H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
Goal 2 - Processes exist to minimize barriers to the Insider Risk Mitigation Team's access to relevant information in an efficient and secure manner.				
1.	Has senior or executive management directed components of the organization to provide data sources and other information to the Insider Risk Mitigation Team that are necessary to identify, analyze, and resolve insider risk matters?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.DP-4:** Event detection information is communicated	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Are data sources and other relevant information provided in a secure manner?	**PR.DS-1:** Data-at-rest is protected **PR.DS-2:** Data-in-transit is protected **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition **PR.DS-5:** Protections against data leaks are implemented **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
3.	Are data sources and other relevant information provided in a timely manner, according to organizational requirements?	**PR.DS-4:** Adequate capacity to ensure availability is maintained	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
4.	Are procedures established for the Insider Risk Mitigation Team to request access to organizational components that maintain or handle sensitive or protected information?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
5.	Does the organization have guidelines for all components – such as IT and HR -- to report information about insider threats directly to the Insider Risk Team?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **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	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
6.	Does the Insider Risk Mitigation Team have timely access to analytic products pertaining to adversarial threats, based on organizational requirements?	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **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)	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
7.	Are all information-sharing activities conducted in accordance with applicable laws, whistleblower protections, civil liberties, and privacy policies?	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
8.	Are new data sources reviewed for applicability to the Insider Risk Mitigation Program?	**DE.DP-5:** Detection processes are continuously improved	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
9.	Do documented policies and procedures specify the processes and mechanisms used by the Insider Risk Mitigation Team to gain access to new data sources?	**DE.DP-5:** Detection processes are continuously improved	(2) Develop a formalized Insider Risk program. (22) Learn from past insider threat incidents.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Human Resources, Incident Management, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 3 - Relevant organizational components securely provide the Insider Risk Mitigation Team with the information necessary to detect, identify, assess, and manage insider threat activities.			
1. Is the data that must be sent to the Insider Risk Mitigation Team or for which access is to be allowed defined in policy or guidance?	**DE.DP-2:** Detection activities comply with all applicable requirements	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2. Does data reported to the Insider Risk Mitigation Team or for which access is allowed include the following categories? • Personnel usernames • Levels of network access • Audit data • Unauthorized use of removable media • Print logs	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
3. Does data reported to the Insider Risk Mitigation Team or for which access is allowed include incident reports?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 4 - The organization monitors user activity on its networks and systems to identify concerning behaviors that are within the scope of the Insider Risk Program.			
1. Does the Insider Risk Mitigation Team have access to the necessary user activity data on its networks and systems to allow it to identify concerning behaviors that are within the scope of the Insider Risk Program?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **RS.AN-1:** Notifications from detection systems are investigated	(11) Institute stringent access controls and monitoring policies on privileged users. (12) Deploy solutions for monitoring employee actions and correlating information from multiple data sources. (13) Monitor remote access from all end points, including mobile devices. (14) Establish a baseline of normal behavior for both networks and employees.	• NIST SP 800-53 Rev. 5 AC-17, AC-19, AC-2, AC-20, AC-3, AC-4, AC-6, AU-1, AU-12, AU-2, AU-3, AU-5, AU-6, AU-7, AU-9, CA-3, CA-6, CM-11, CM-12, CM-3, CM-5, CM-7, IA-12, IA-2, IR-3, IR-4, IR-8, MA-3, MA-5, MA-7, PE-3, PL-4, PM-21, PM-31, PS-3, PT-2, PT-3, RA-3, RA-4, SA-5, SA-8, SA-9, SC-45, SC-46, SC-48, SC-7, SI-10, SI-4, SR-3, SR-4, SR-5 • National Insider Threat Policy C-1-1, C-1-2, C-1-4 • Minimum Standards E-1, H-1 • CERT-RMM Identity/Access Management, Monitoring, Technology Management • CIS CSC 4, 6 • CMMC AC.1.001, AC.1.002, AC.2.013, AC.2.015, AC.3.014, AC.3.020, AC.3.021, AC.3.022, AU.2.041, AU.2.042, AU.3.045, AU.3.049, AU.3.050, AU.3.052, AU.5.055, CM.2.062, CM.3.067, CM.3.068, CM.3.069, CM.4.073, IA.1.076, IA.1.077, IA.3.083, IA.3.084, IR.2.097, IR.5.106, MA.2.114, SC.1.175, SC.1.176, SC.3.183, SC.3.184, SC.5.230

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Goal 5 - The organization has an insider risk analytic capability to gather, review, and analyze information for concerning behaviors that are within the scope of the Insider Risk Program.			
1. Is there a defined and established insider risk analytic capability?	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **ID.GV-4:** Governance and risk management processes address cybersecurity risks **ID.RA-3:** Threats, both internal and external, are identified and documented	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2. Have analysts been identified and trained to perform required insider threat analytical activities?	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **RS.AN-1:** Notifications from detection systems are investigated	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
3. Does the analytical capability sufficiently allow for the integration, review, and assessment of user activity to identify concerning behaviors that are within the scope of the Insider Risk Program?	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **RS.AN-1:** Notifications from detection systems are investigated	(2) Develop a formalized Insider Risk program.	• NIST SP 800-53 Rev. 5 AT-2, AU-6, CM-11, CM-12, CM-3, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-10, SA-8, SC-16, SC-48, SI-18, SI-4, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Goal 6 - The Insider Risk Mitigation Team leverages employee background screening data.			
1. Is there a defined process in place for sharing background screening data about an employee with the Insider Risk Program (if applicable)?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	• NIST SP 800-53 Rev. 5 AU-12, PS-1, PS-2, PS-3, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
2. Are there thresholds for sharing employee background screening data with the Insider Risk Program when potential incidents or escalations require them?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	(4) Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	• NIST SP 800-53 Rev. 5 AU-12, PS-1, PS-2, PS-3, PS-8, SR-1 • National Insider Threat Policy C-1-1, C-1-2 • Minimum Standards H • CERT-RMM Human Resources, Monitoring • CMMC PS.2.127
Goal 7- The Insider Risk Mitigation Team supports the employee separation processes.			
1. Is there a defined process in place for notifying the Insider Risk Program when an employee is going to separate (or be separated from) the organization?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	(20) Develop a comprehensive employee termination procedure.	• NIST SP 800-53 Rev. 5 PS-4, PS-5 • Minimum Standards G-1-c • CERT-RMM Human Resources • CIS CSC 16 • CMMC PS.2.128 •

	Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
2.	Is there a formal or written procedure with accountability for compliance by which the Insider Risk Program is notified in a timely manner when an employee is going to separate (or be separated from) the organization?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	(20) Develop a comprehensive employee termination procedure.	• NIST SP 800-53 Rev. 5 PS-4, PS-5 • Minimum Standards G-1-c • CERT-RMM Human Resources • CIS CSC 16 • CMMMC PS.2.128
3.	Is there a defined offboarding process in place for separating employees that includes affirmation of continuing adherence to insider risk training, non-disclosure agreements, etc.?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	(20) Develop a comprehensive employee termination procedure.	• NIST SP 800-53 Rev. 5 PS-4, PS-5 • Minimum Standards G-1-c • CERT-RMM Human Resources • CIS CSC 16 • CMMMC PS.2.128
Goal 8 - The Insider Risk Mitigation Team can distinguish between acceptable and unacceptable employee behavior.				
1.	Does the Insider Risk Program incorporate the organization's policies that define acceptable and unacceptable workplace behavior into its analytical capabilities?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.AE-5:** Incident alert thresholds are established **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **DE.DP-2:** Detection activities comply with all applicable requirements	(14) Establish a baseline of normal behavior for both networks and employees.	• NIST SP 800-53 Rev. 5 AC-17, AU-12, CA-3, CM-7, IR-3, IR-4, IR-8, PM-31, RA-4, SA-8, SC-46, SC-48, SC-7, SI-4, SR-3 • National Insider Threat Policy C-1-2 • Minimum Standards E-1 • CERT-RMM Monitoring • CIS CSC 6 • CMMC AC.1.001, AC.1.002, AC.2.013, AC.2.015, AC.3.014, AC.3.021, CM.2.062, CM.3.068, CM.3.069, CM.4.073, SC.1.175, SC.1.176, SC.3.183, SC.3.184, SC.5.230
Maturity Indicator Level (MIL) 2 - Planned				
1.	Is there a plan for performing data collection and analysis activities?	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **DE.DP-2:** Detection activities comply with all applicable requirements	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Is there a documented policy for data collection and analysis activities?			
3.	Have stakeholders for data collection and analysis activities been identified and made aware of their roles?			
4.	Have data collection and analysis standards and guidelines been identified and implemented?			
Maturity Indicator Level (MIL) 3 - Managed				
1.	Is there oversight of data collection and analysis activities?	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
2.	Have qualified staff been assigned to perform data collection and analysis activities?			
3.	Is there adequate funding to perform data collection and analysis activities as planned?			
4.	Are risks related to the performance of planned data collection and analysis activities identified, analyzed, disposed of, monitored, and controlled?			

Question	NIST CSF Reference(s)	*Common Sense Guide to Managing Insider Risk* Best Practice(s)	*Common Sense Guide to Managing Insider Risk* Cybersecurity Framework References
Maturity Indicator Level (MIL) 4 – Measured			
1. Are data collection and analysis activities periodically reviewed and measured to ensure they are effective and producing intended results? Are data collection and analysis activities periodically reviewed to ensure they are adhering to the plan? Is higher-level management aware of issues related to the performance of data collection and analysis?	**DE.DP-3:** Detection processes are tested **DE.DP-5:** Detection processes are continuously improved	(2) Develop a formalized Insider Risk program. (17) Institutionalize system change controls.	• NIST SP 800-53 Rev. 5 AC-4, AT-2, AU-6, CA-7, CM-1, CM-3, CM-4, CM-5, CM-6, CM-11, CM-12, CM-13, IR-2, IR-4, PM-19, PM-23, PM-29, PM-31, PT-7, RA-8, RA-10, SA-8, SA-10, SC-16, SC-48, SI-4, SI-18, SR-2, SR-4, SR-6, SR-8, SR-9, SR-10, SR-11 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Incident Management and Control, Technology Management, Vulnerability Analysis and Resolution • CIS CSC 3, 5, 11 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CM.2.061, CM.2.064, CM.2.065, CM.2.066, CM.3.067, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217
Maturity Indicator Level (MIL) 5 - Defined			
1. Has the organization adopted a standard definition of data collection and analysis activities from which operating units can derive practices that fit their unique operating circumstances? 2. Are improvements to the program's data collection and analysis activities documented and shared across the organization?	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	(2) Develop a formalized Insider Risk program. (3) Clearly document and consistently enforce policies and controls.	• NIST SP 800-53 Rev. 5 AC-12, AC-20, AC-3, AT-2, AU-6, CA-7, CM-11, CM-12, CM-3, IR-2, IR-3, IR-4, IR-8, PE-3, PL-1, PL-4, PM-17, PM-19, PM-22, PM-23, PM-27, PM-29, PM-31, PS-8, PS-9, PT-1, PT-6, PT-7, RA-10, SA-10, SA-17, SA-8, SC-16, SC-48, SC-7, SC-8, SI-18, SI-4, SR-1, SR-10, SR-2, SR-4, SR-6, SR-8, SR-9 • National Insider Threat Policy B • Minimum Standards G-1 • CERT-RMM Compliance, Incident Management and Control, Vulnerability Analysis and Resolution • CIS CSC 3, 6 • CMMC AC.5.024, AT.2.056, AU.2.041, AU.4.053, CA.4.163, IR.2.092, IR.2.094, IR.2.096, IR.5.102, SA.4.173, SI.2.216, SI.2.217

References

Center for Internet Security Controls, 2019. *CIS Controls Version 7.1*. retrieved July 20, 2021, from https://www.cisecurity.org/controls/v7/

Office of the Director of National Intelligence, 2012. *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. Retrieved July 20, 2021, from https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

Software Engineering Institute, Carnegie Mellon University. 2016. *CERT Resilience Management Model (CERT-RMM), Version 1.2*. Retrieved July 20, 2021, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Software Engineering Institute, Carnegie Mellon University. 2019. *Common Sense Guide to Managing Insider Risk, Sixth Edition*. Retrieved July 20, 2021, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

U. S. Department of Commerce, National Institute of Standards and Technology (NIST), *NIST Cybersecurity Framework, Version 1.1*, 2018. Retrieved July 20, 2021, from https://www.nist.gov/cyberframework

U. S. Department of Commerce, National Institute of Standards and Technology (NIST), 2020. *Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5*. Retrieved July 20, 2021, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

U. S. Department of Defense, 2020.*Cybersecurity Maturity Model Certification (CMMC), Version 1.02*. Retrieved July 20, 2021, from https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY