INCIDENT MANAGEMENT REVIEW (IMR)

NIST Cybersecurity Framework Crosswalks

SEPTEMBER 2023

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

This material is based upon work funded and supported by the Department of Defense 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.

DM20-0605

Table of 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.

The 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 Incident Management Review (IMR) Crosswalk

NIST Cybersecurity Framework (CSF) Reference Keys

Identifier	Function	Identifier	Category
ID	Identity	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	[Response] Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	[Response] Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	{Recovery] Improvements
		RC.CO	[Recovery] Communication

Incident Management Review (IMR) Reference Keys

Identifier	Domain
EH	Event Detection and Handling
IR	Incident Declaration, Handling and Response
PI	Post-Incident Analysis and Testing
OC	Integration of Organizational Capabilities
PS	Protection and Sustainment of the Incident Management Function
PR	Preparation for Incident Response
G	Goal
Q	Question

NOTE:

- NIST CSF references are formatted as **NIST CSF Function.Category-Subcategory Number**. For example, **ID.AM-1** means **Identity** (ID) function, **Asset Management** (AM) category, subcategory **one** (1).
- IMR references are formatted as **IMR Domain:Goal Number.Question Number**. For example, **EH:G3.Q5** means **Event Handing** (EH) domain, goal **three** (G3), question **five** (Q5).
- References for the IMR questions can be found in the IMR to NIST CSF Crosswalk starting on page 18.

Identify (ID)

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. IMR References EH:G1.Q3 EH:G1.Q4 PS:G1.Q1	**ID.AM-1**: Physical devices and systems within the organization are inventoried.	EH:G1.Q3 EH:G1.Q4 PS:G1.Q1	• 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.	EH:G1.Q3 EH:G1.Q4 PS:G1.Q1	• 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.	EH:G1.Q3 EH:G1.Q4	• 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.	EH:G1.Q3 EH:G1.Q4 PS:G1.Q1	• 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.	EH:G1.Q2	• CIS CSC 13, 14 • COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	PR:G1.Q5	• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Identify (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. IMR References EH:G1.Q1 EH:G1.Q2	**ID.BE-1**: The organization's role in the supply chain is identified and communicated.	PR:G4.Q2 PR:G4.Q3	• 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.		• 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.		• 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.	EH:G1.Q3 EH:G1.Q4 PR:G4.Q1	• 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).	EH:G1.Q3 EH:G1.Q4 PS:G1.Q2	• 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
	Governance (ID.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.		• 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.	PR:G1.Q5	• 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.	IR:G4.Q1 IR:G4.Q2 IR:G4.Q3 PS:G1.Q3	• 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.	PS:G1.Q3	• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Identify (ID)	**Risk Assessment (ID.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.	OC:G2.Q1 OC:G2.Q2 PS:G1.Q10	• 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.	OC:G4.Q1	• 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.	OC:G4.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.		• 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.		• 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.		• CIS CSC 4 • COBIT 5 APO12.05, APO13.02 • ISO/IEC 27001:2013 Clause 6.1.3 • NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (ID.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.		• 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.		• 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.		• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Identify (ID)	**Supply Chain Risk Management (ID.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.		• 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.	PR:G4.Q1	• 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.	PR:G4.Q2 PR:G4.Q3	• 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.	PR:G4.Q4	• COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • ISA 62443-2-1:2009 4.3.2.6.7 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	PI:G2.Q1 PI:G2.Q2 PI:G2.Q3 PI:G2.Q4 PI:G2.Q5 PI:G2.Q6 PS:G1.Q6 PS:G2.Q3 PR:G1.Q1 PR:G1.Q2 PR:G1.Q6 PR:G1.Q7 PR:G2.Q1 PR:G2.Q2	• 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	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)	**Identity Management, Authentication and Access Control (PR.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. IMR References: PS:G1.Q3	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.		• 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.	PS:G1.Q7	• 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.		• CIS CSC 12 • COBIT 5 AP013.01, 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.	PS: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).		• 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.		• CIS CSC, 16 • COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 • ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)		**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).		• CIS CSC 1, 12, 15, 16 • COBIT 5 DSS05.04, DSS05.10, DSS06.10 • ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.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.	PR:G5.Q1 PR:G5.Q2 PR:G5.Q3	• CIS CSC 17, 18 • COBIT 5 AP007.03, 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.		• CIS CSC 5, 17, 18 • COBIT 5 AP007.02, 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.	PR:G4.Q2 PR:G4.Q3	• CIS CSC 17 • COBIT 5 AP007.03, AP007.06, AP010.04, AP010.05 • 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.	PR:G1.Q5	• CIS CSC 17, 19 • COBIT 5 EDM01.01, AP001.02, AP007.03 • 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.		• CIS CSC 17 • COBIT 5 AP007.03 • 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 (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. IMR References: PS:G1.Q3	**PR.DS-1:** Data-at-rest is protected.		• CIS CSC 13, 14 • COBIT 5 AP001.06, 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)		**PR.DS-2:** Data-in-transit is protected.		• 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.	PS:G2.Q1	• 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.		• 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.		• CIS CSC 13 • COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.		• 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.		• 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.		• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. IMR References: PS:G1.Q3	**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).		• 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.	PS:G1.Q5	• 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.	OC:G1.Q1 OC:G1.Q2 PS:G1.Q4 PS:G2.Q4	• 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.	PS:G2.Q1 PS:G2.Q2 PS:G2.Q3	• 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.		• 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.	PS:G2.Q1	• 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.	IR:G2.Q5 PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5 PR:G5.Q1	• 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	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)		**PR.IP-8:** Effectiveness of protection technologies is shared.	OC:G4.Q2	• 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.	OC:G3.Q1 OC:G3.Q2 PS:G1.Q6 PS:G1.Q9 PR:G1.Q1 PR:G1.Q6 PR:G1.Q7 PR:G2.Q1 PR:G2.Q2	• CIS CSC 19 • COBIT 5 AP012.06, 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.	PI:G2.Q1 PI:G2.Q2 PI:G2.Q3 PI:G2.Q4 PI:G2.Q5 PI:G2.Q6 PR:G1.Q2	• 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).	EH:G3.Q7 PS:G2.Q4 PR:G1.Q4	• CIS CSC 5, 16 • COBIT 5 AP007.01, AP007.02, AP007.03, AP007.04, AP007.05 • 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.		• 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 (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. IMR References: PS:G1.Q3	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.		• 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.		• CIS CSC 3, 5 • COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Protect (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. IMR References: PS:G1.Q3	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.		• CIS CSC 1, 3, 5, 6, 14, 15, 16 • COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected, and its use restricted according to policy.		• 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.		• 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.		• 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.		• 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	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Detect (DE)	**Anomalies and Events (DE.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.		• 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.	EH:G3.Q2 EH:G3.Q3	• CIS CSC 3, 6, 13, 15 • COBIT 5 DSS05.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	EH:G2.Q2 EH:G3.Q2 EH:G3.Q3 EH:G3.Q5 EH:G3.Q6	• 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.	EH:G3.Q4	• 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.	IR:G1.Q2	• CIS CSC 6, 19 • COBIT 5 APO12.06, DSS03.01 • ISA 62443-2-1:2009 4.2.3.10 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.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.	EH:G1.Q5 EH:G1.Q6 EH:G2.Q1 PS:G1.Q8	• 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.	EH:G1.Q5 EH:G1.Q6 EH:G2.Q1	• 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.	EH:G1.Q5 EH:G1.Q6 EH:G2.Q1	• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Detect (DE)		**DE.CM-4:** Malicious code is detected.		• 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.		• 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.		• COBIT 5 APO07.06, APO10.05 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.		• 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.	PS:G1.Q10	• 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 (DE.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.	EH:G3.Q7 PS:G1.Q9 PR:G1.Q1 PR:G1.Q3 PR:G1.Q4 PR:G1.Q6 PR:G2.Q1	• 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.	EH:G3.Q7 IR:G4.Q1 IR:G4.Q2	• 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.		• 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.	EH:G1.Q7 EH:G2.Q1	• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Detect (DE)		**DE.DP-5:** Detection processes are continuously improved.	IR:G2.Q5 PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5 PR:G1.Q2	• 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	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Respond (RS)	**Response Planning (RS.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.	IR:G3.Q4 PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5	• 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 (RS.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.	EH:G3.Q7 PR:G1.Q1 PR:G1.Q3 PR:G1.Q6 PR:G2.Q1	• 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.	EH:G1.Q7 EH:G2.Q3 IR:G1.Q1 IR:G3.Q2 IR:G3.Q3	• 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.	IR:G3.Q2 IR:G3.Q3 IR:G3.Q5 IR:G3.Q6 IR:G4.Q4 PR:G3.Q1 PR:G3.Q2	• 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.	IR:G1.Q3 IR:G3.Q1 PR:G1.Q1 PR:G1.Q6 PR:G2.Q1	• 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.	OC:G4.Q2	• 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 (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	EH:G3.Q6	• 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.	IR:G2.Q1 IR:G2.Q2 IR:G2.Q3 IR:G2.Q4	• 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

Function	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Respond (RS)		**RS.AN-3:** Forensics are performed.	IR:G4.Q3	• COBIT 5 APO12.06, DSS03.02, DSS05.07 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans.	EH:G3.Q1 IR:G2.Q1 IR:G2.Q2 IR:G2.Q3	• 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).	OC:G2.Q1 OC:G2.Q2 OC:G2.Q3 PS:G1.Q10	• CIS CSC 4, 19 • COBIT 5 EDM03.02, DSS05.07 • NIST SP 800-53 Rev. 4 SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained.	IR:G3.Q4 IR:G3.Q7	• 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.	IR:G3.Q7	• 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.		• 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 (RS.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.	PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5	• 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.	PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5	• 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	CSF Category	CSF Subcategory	IMR References	Informative References for NIST CSF
Recover (RC)	**Recovery Planning (RC.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.		• 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 (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned.	PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5	• 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.	PI:G1.Q1 PI:G1.Q2 PI:G1.Q3 PI:G1.Q4 PI:G1.Q5	• 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 (RC.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.	IR:G3.Q5 IR:G3.Q6 PR:G3.Q1 PR:G3.Q2	• COBIT 5 EDM03.02 • ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident.		• 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.	IR:G3.Q5 IR:G3.Q6 IR:G4.Q4 PR:G3.Q1 PR:G3.Q2	• COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4

Incident Management Review (IMR) to NIST Cybersecurity Framework (CSF) Crosswalk

Incident Management Review (IMR) Reference Keys

Identifier	Domain
EH	Event Detection and Handling
IR	Incident Declaration, Handling and Response
PI	Post-Incident Analysis and Testing
OC	Integration of Organizational Capabilities
PS	Protection and Sustainment of the Incident Management Function
PR	Preparation for Incident Response
G	Goal
Q	Question

NIST Cybersecurity Framework (CSF) Reference Keys

Identifier	Function	Identifier	Category
ID	Identity	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	[Response] Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	[Response] Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	{Recovery] Improvements
		RC.CO	[Recovery] Communication

NOTE:

- IMR references are formatted as **IMR Domain:Goal Number.Question Number**. For example, **EH:G3.Q5** means **Event Handing** (EH) domain, goal **three** (G3), question **five** (Q5).
- NIST CSF references are formatted as **NIST CSF Function.Category-Subcategory Number**. For example, **ID.AM-1** means **Identity** (ID) function, **Asset Management** (AM) category, subcategory **one** (1).
- References for the NIST CSF functions and categories can be found in the NIST CSF to IMR Crosswalk starting on page 1.

1 Event Detection and Handling

Domain	IMR Assessment		NIST CSF References	Notes
Event Detection and Handling (EH)	**1 Event Detection and Handling (EH)** The purpose of Event Detection and Handling is to detect, report, analyze, manage, and track events to resolution.			
	Goal 1—Organizational services and assets are prioritized and supported by event detection and handling capabilities.			
	1.	Are the Organization's Critical Services identified?	**ID.BE:** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The concept of a service is not directly addressed. Services support the organizational mission, and therefore, the question is mapped to the NIST CSF category of ID.BE.
	2.	Are the organization's services prioritized, in order to focus event detection and incident response efforts on high-priority systems and assets?	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value. **ID.BE:** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	3.	Are the high-value assets (technology, information, people, and facilities) that directly support the organization's critical services inventoried?	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. **ID.AM-1:** Physical devices and systems within the organization are inventoried. **ID.AM-2:** Software platforms and applications within the organization are inventoried. **ID.AM-3:** Organizational communication and data flows are mapped. **ID.AM-4:** External information systems are catalogued. **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established. **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	
	4.	Do event detection and incident handling and response personnel have access to an organizational asset inventory?	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. **ID.AM-1:** Physical devices and systems within the organization are inventoried. **ID.AM-2:** Software platforms and applications within the organization are inventoried. **ID.AM-3:** Organizational communication and data flows are mapped. **ID.AM-4:** External information systems are catalogued. **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established. **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	

Domain	IMR Assessment		NIST CSF References	Notes
Event Detection and Handling (EH)	5.	Has the organization implemented security monitoring activities?	**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.	
	6.	Are the assets (people, information, technology, and facility) supporting those critical services monitored by the organization's security monitoring activities?	**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.	
	7.	Are events from those security monitoring activities reported to the Incident Management Function?	**DE.DP-4:** Event detection information is communicated. **RS.CO-2:** Incidents are reported consistent with established criteria.	
	Goal 2—Events are detected.			
	1.	Are events detected and reported?	**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.	
	2.	Is event data logged in an incident knowledgebase or similar mechanism?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.	
	3.	Does guidance exist that defines the types of events and incidents that should be reported (by users or partners)?	**RS.CO-2:** Incidents are reported consistent with established criteria.	
	Goal 3— Events are analyzed, processed, and tracked.			
	1.	Are events categorized?	**RS.AN-4:** Incidents are categorized consistent with response plans.	
	2.	Are events analyzed to determine if they are related to other events?	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods. **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.	
	3.	Is there a standard set of tools and/or methods in use to perform event correlation?	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods. **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.	
	4.	Are events prioritized?	**DE.AE-4:** Impact of events is determined.	
	5.	Is the status of events tracked?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.	
	6.	Are events managed and tracked to resolution?	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors. **RS.AN-1:** Notifications from detection systems are investigated.	

Domain	IMR Assessment		NIST CSF References	Notes
Event Detection and Handling (EH)	7.	Are staff held accountable for performing event management on assets that support the organization's critical services?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability. **DE.DP-2:** Detection activities comply with all applicable requirements. **RS.CO-1:** Personnel know their roles and order of operations when a response is needed.	

2 Incident Declaration, Handling, and Response

Domain	IMR Assessment		NIST CSF References	Notes
Incident Declaration, Handling, and Response (IR)	**2 Incident Declaration, Handling, and Response (IR)** The purpose of Incident Declaration, Handling, and Response is to declare, analyze, respond, manage, and track incidents to resolution.			
	Goal 1—Incidents are declared.			
	1.	Are incidents declared in accordance with a documented process?	**RS.CO-2:** Incidents are reported consistent with established criteria.	
	2.	Have criteria for the declaration of an incident been established?	**DE.AE-5:** Incident alert thresholds are established.	
	3.	Is there a process to prioritize and transfer incidents to the appropriate queue, group, or personnel after formal incident declaration?	**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.	
	Goal 2—Incidents are analyzed and correlated to determine a response.			
	1.	Are incidents analyzed to determine a response?	**RS.AN-2:** The impact of the incident is understood. **RS.AN-4:** Incidents are categorized consistent with response plans.	
	2.	Are incidents analyzed to determine if they are related to other incidents or events?	**RS.AN-2:** The impact of the incident is understood. **RS.AN-4:** Incidents are categorized consistent with response plans.	
	3.	Is there a standard set of tools and/or methods in use to perform incident correlation?	**RS.AN-2:** The impact of the incident is understood. **RS.AN-4:** Incidents are categorized consistent with response plans.	
	4.	Is the impact to the organization's services assessed in the course of incident analysis?	**RS.AN-2:** The impact of the incident is understood.	
	5.	Is analysis performed to determine the root causes of incidents?	**PR.IP-7:** Protections against data leaks are implemented. **DE.DP-5:** Detection processes are continuously improved.	
	Goal 3—Incident response is implemented.			
	1.	Are incidents escalated to internal and external stakeholders for input and resolution?	**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.	
	2.	Does guidance exist that includes the categories of incidents to report, along with the required information, timeframes, and contact mechanisms for internal and external stakeholders?	**RS.CO-2:** Incidents are reported consistent with established criteria. **RS.CO-3:** Information is shared consistent with response plans.	

Domain	IMR Assessment		NIST CSF References	Notes
	3.	Does the guidance include operational and information security requirements?	**RS.CO-2:** Incidents are reported consistent with established criteria. **RS.CO-3:** Information is shared consistent with response plans.	
Incident Declaration, Handling, and Response (IR)	4.	Are responses to declared incidents developed and implemented according to pre-defined procedures?	**RS.RP-1:** Response plan is executed during or after an incident. **RS.MI-1:** Incidents are contained.	
	5.	Are incident status and response communicated to affected parties (including public relations staff and external media outlets)?	**RS.CO-3:** Information is shared consistent with response plans. **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.	
	6.	Are alerts and warnings applicable to ongoing incidents communicated to the internal and external stakeholders as necessary?	**RS.CO-3:** Information is shared consistent with response plans. **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.	
	7.	Are incidents managed and tracked to resolution?	**RS.MI-1:** Incidents are contained. **RS.MI-2:** Incidents are mitigated.	
	Goal 4—Forensic handling of events and incidents is conducted.			
	1.	Have requirements (rules, laws, regulations, policies, etc.) for identifying event and incident evidence for forensic purposes been identified?	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. **DE.DP-2:** Detection activities comply with all applicable requirements.	
	2.	Have criteria been defined for when forensic analysis should be conducted on events and incidents?	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. **DE.DP-2:** Detection activities comply with all applicable requirements.	
	3.	Is there a documented process to ensure event and incident evidence is handled and retained in accordance with the organization's legal or regulatory obligations, or in accordance with the needs of law enforcement or other incident responders?	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. **RS.AN-3:** Forensics are performed.	
	4.	Are forensic analysis results and reports provided to the appropriate stakeholders?	**RS.CO-3:** Information is shared consistent with response plans. **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	

3 Post-Incident Analysis and Testing

Domain	IMR Assessment		NIST CSF References	Notes
Post-Incident Analysis and Testing (PI)	**3 Post-Incident Analysis and Testing (PI)** The purpose of Post-Incident Analysis and Testing is to capture lessons learned to improve the incident detection, handling, or response capability, and other organizational protection and sustainment strategies.			
	Goal 1—Post-incident review and analysis is conducted as appropriate.			
	1.	Do criteria exist for identifying incidents that require a post-incident review?	**PR.IP-7:** Protection processes are improved. **DE.DP-5:** Detection processes are continuously improved. **RS.RP-1:** Response plan is executed during or after an incident. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated. **RC.IM-1:** Recovery plans incorporate lessons learned. **RC.IM-2:** Recovery strategies are updated.	
	2.	Is a post-incident review performed?	**PR.IP-7:** Protection processes are improved. **DE.DP-5:** Detection processes are continuously improved. **RS.RP-1:** Response plan is executed during or after an incident. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated. **RC.IM-1:** Recovery plans incorporate lessons learned. **RC.IM-2:** Recovery strategies are updated.	
	3.	Are lessons learned from post-incident review and analysis used to improve organizational asset protection and sustainment strategies?	**PR.IP-7:** Protection processes are improved. **DE.DP-5:** Detection processes are continuously improved. **RS.RP-1:** Response plan is executed during or after an incident. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated. **RC.IM-1:** Recovery plans incorporate lessons learned. **RC.IM-2:** Recovery strategies are updated.	

Domain		IMR Assessment	NIST CSF References	Notes
Post-Incident Analysis and Testing (PI)	4.	Are improvements to the event and incident detection, handling or response process identified as a result of post-incident review and analysis?	**PR.IP-7:** Protection processes are improved. **DE.DP-5:** Detection processes are continuously improved. **RS.RP-1:** Response plan is executed during or after an incident. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated. **RC.IM-1:** Recovery plans incorporate lessons learned. **RC.IM-2:** Recovery strategies are updated.	
	5.	Are post-incident analysis reports generated and archived?	**PR.IP-7:** Protection processes are improved. **DE.DP-5:** Detection processes are continuously improved. **RS.RP-1:** Response plan is executed during or after an incident. **RS.IM-1:** Response plans incorporate lessons learned. **RS.IM-2:** Response strategies are updated. **RC.IM-1:** Recovery plans incorporate lessons learned. **RC.IM-2:** Recovery strategies are updated.	
	Goal 2—The incident detection, handling, and response capability is tested and exercised.			
	1.	Have standards for testing the incident detection, handling, and response process been implemented?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	
	2.	Does documented guidance exist that requires periodic testing of the incident detection, handling, and response activities?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	
	3.	Has a schedule for testing the incident detection, handling, and response process been established?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	
	4.	Is the incident detection, handling, and response process tested?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	
	5.	Are all relevant elements of the organization involved in testing the incident detection, handling, and response processes?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	

Domain	IMR Assessment		NIST CSF References	Notes
Post-Incident Analysis and Testing (PI)	6.	Are test results compared with test objectives to identify needed improvements to the incident detection, handling, and response processes?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested.	

4 Integration of Organizational Capabilities

Domain	IMR Assessment		NIST CSF References	Notes
Integration of Organizational Capabilities (OC)	**4 Integration of Organizational Capabilities (OC)** The purpose of integrating the incident detection, handling, and response processes with the organization's cyber resilience activities is to enable the organization to effectively respond to incidents.			
	Goal 1— The Incident Management Function is integrated with the organization's change management program.			
	1.	Does the organization have a change management process that is used to manage modifications to assets?	**PR.IP-3:** Configuration change control processes are in place.	
	2.	Are event and incident handling personnel notified of upcoming changes to organizational assets?	**PR.IP-3:** Configuration change control processes are in place.	
	Goal 2—The Incident Management Function is able to leverage the organization's vulnerability analysis and resolution activities.			
	1.	Does the organization use a repository for recording information about vulnerabilities and their resolutions?	**ID.RA-1:** Asset vulnerabilities are identified and documented. **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.	Do event and incident handling personnel have access to an up-to-date vulnerability management repository?	**ID.RA-1:** Asset vulnerabilities are identified and documented. **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).	
	3.	Are the event and incident handling personnel notified when unmitigated vulnerabilities exist, or where compensating controls may need to be monitored?	**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).	
	Goal 3—Incident Management Function is integrated with the organization's service continuity program.			
	1.	Is the Incident Management Function properly integrated in all organizational service continuity plans?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	2.	Are the organization's service continuity plans periodically reviewed and updated to ensure proper inclusion of the Incident Management Function?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	Goal 4—Incident Management Function is integrated with the organization's threat monitoring program.			
	1.	Has the organization implemented a threat monitoring capability?	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources. **ID.RA-3:** Threats, both internal and external, are identified and documented.	

Domain	IMR Assessment		NIST CSF References	Notes
Integration of Organizational Capabilities (OC)	2.	Is relevant threat information communicated to the Incident Management Function?	**PR.IP-8:** Effectiveness of protection technologies is shared. **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	

5 Protection and Sustainment of the Incident Management Function

Domain	IMR Assessment		NIST CSF References	Notes
Protection and Sustainment of the Incident Management Function (PS)	**5 Protection and Sustainment of the Incident Management Function (PS)** The purpose of protecting and sustaining the Incident Management Function is to ensure the delivery of the incident management activities to the organization.			
	Goal 1—The Incident Management Function's assets are protected and sustained.			
	1.	Are the assets that directly support the Incident Management Function inventoried?	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. **ID.AM-1:** Physical devices and systems within the organization are inventoried. **ID.AM-2:** Software platforms and applications within the organization are inventoried. **ID.AM-4:** External information systems are catalogued.	
	2.	Do Incident Management Function asset descriptions include protection and sustainment requirements?	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress and/or attack, during recovery, normal operations).	
	3.	Are controls established to protect and sustain the Incident Management Function at a level equal to or greater than those established for the organization's other critical assets?	**Identity Management, Authentication, and Access Control (PR.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. **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets in a manner consistent with related policies, procedures, and agreements. **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. **ID.GV-4:** Governance and risk management processes address cybersecurity risks.	
	4.	Is a change management process used to manage modifications to assets (technology, information, and facilities) that directly support the Incident Management Function?	**PR.IP-3:** Configuration change control processes are in place.	
	5.	Do documented procedures exist for defining tool requirements, and for acquiring, developing, deploying, and maintaining tools (e.g., a System Development Life Cycle)?	**PR.IP-2:** A System Development Life Cycle to manage systems is implemented.	

Domain	IMR Assessment		NIST CSF References	Notes
Protection and Sustainment of the Incident Management Function (PS)	6.	Are service continuity plans developed and documented for assets required for the delivery of the Incident Management Function activities?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	7.	Are physical protection measures established and managed for assets that directly support the Incident Management Function?	**PR.AC-2:** Physical access to assets is managed and protected.	
	8.	Are Incident Management Function systems and networks monitored by the organization's security monitoring activities?	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	
	9.	Are event detection and incident response activities performed on the assets that directly support the Incident Management Function?	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.	
	10.	Is vulnerability management performed on the assets that directly support the Incident Management Function?	**ID.RA-1:** Asset vulnerabilities are identified and documented. **DE.CM-8:** Vulnerability scans are performed. **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	
	Goal 2—The confidentiality, integrity and availability of event and incident information is managed.			
	1.	Do guidelines exist for the secure collection, handling, transmission, storage, retention, and destruction of event and incident data?	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition. **PR.IP-4:** Backups of information are conducted, maintained, and tested. **PR.IP-6:** Data is destroyed according to policy.	
	2.	Are event and incident information assets backed up and retained?	**PR.IP-4:** Backups of information are conducted, maintained, and tested.	
	3.	Are backup, storage, and restoration procedures for event and incident information assets tested?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-4:** Backups of information are conducted, maintained, and tested.	
	4.	Are integrity requirements used to determine which staff members are authorized to modify event and incident information?	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. **PR.IP-3:** Configuration change control processes are in place. **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	

6 Preparation for Incident Response

Domain	IMR Assessment		NIST CSF References	Notes
Preparation for Incident Response (PR)	**6 Preparation for Incident Response (PR)** The purpose of preparing for incident response is to define and establish a capability for event detection and incident handling and response to respond to incidents that have an impact on the organization's mission.			
	Goal 1—A process to detect and analyze events, identify incidents, and determine an organizational response is established.			
	1.	Does the organization have an incident management plan for detecting and triaging events, and for handling and responding to incidents?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. **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. **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.	
	2.	Is the incident management plan reviewed and updated according to a pre-planned schedule?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-10:** Response and recovery plans are tested. **DE.DP-5:** Detection processes are continuously improved.	
	3.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan?	**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.	Are employees held accountable for executing the roles and responsibilities detailed in the incident management plan?	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.	
	5.	Has senior leadership been made aware of their roles as outlined in the incident management plan?	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. **PR.AT-4:** Senior executives understand their roles and responsibilities.	
	6.	Have all relevant elements of the organization been involved in creating the incident management plan?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. **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. **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.	

Domain	IMR Assessment		NIST CSF References	Notes
Preparation for Incident Response (PR)	7.	Is a documented workflow in use to ensure the continuity of incident management operations, and the tracking and sharing of data?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	Goal 2—A documented communication plan is established.			
	1.	Has a documented communication plan for incident management activities been established?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. **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. **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.	
	2.	Has the incident management communication plan been disseminated to internal and external stakeholders?	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	Goal 3—Interfaces for the exchange of incident management information are defined.			
	1.	Are there documented information exchange interfaces in use with all internal and external stakeholders?	**RS.CO-3:** Information is shared in a manner consistent with response plans. **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.	For each information exchange interface, are the roles and responsibilities documented for all parties (internal to the organization, and external stakeholders)?	**RS.CO-3:** Information is shared in a manner consistent with response plans. **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.	
	Goal 4—External dependencies on which the Incident Management Function depends are managed.			
	1.	Are dependencies on external relationships that are critical to the Incident Management Function identified?	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established. **ID.SC-2:** Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	
	2.	Are formal agreements, plans, and processes in place for coordinating service delivery between the Incident Management Function and its external dependencies?	**ID.BE-1:** The organization's role in the supply chain is identified and communicated. **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	

Domain	IMR Assessment		NIST CSF References	Notes
Preparation for Incident Response (PR)	3.	Do the formal agreements between the Incident Management Function and its external dependencies require external dependencies to meet the security standards of the organization?	**ID.BE-1:** The organization's role in the supply chain is identified and communicated. **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	
	4.	Has responsibility been assigned for monitoring the performance of external dependencies that support the Incident Management Function?	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
	Goal 5—Incident management personnel are trained.			
	1.	Do knowledge, skill, and ability (KSA) requirements exist for incident handling and response roles?	**PR.AT-1:** All users are informed and trained. **PR.IP-7:** Protection processes are improved.	
	2.	Have training needs for incident handling and response personnel been established?	**PR.AT-1:** All users are informed and trained.	
	3.	Are training activities for the Incident Management Function conducted to meet the identified KSA requirements?	**PR.AT-1:** All users are informed and trained.	

Resources

[Badger 2012]
Badger, L., Grance, T., Patt-Corner, R., Voas, J. *Cloud Computing Synopsis and Recommendations*. National Institute of Standards and Technology Special Publication 800-146, May 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

[Bowen 2006]
Bowen, M., Hash, J., Wilson, M. *Information Security Handbook: A Guide for Managers,* National Institute of Standards and Technology Special Publication 800-100, October 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

[Caralli 2016]
Caralli, R., Allen, J., White, D., Young, L., Mehravari, N., Curtis, P. *CERT Resilience Management Model Version 1.2.* Software Engineering Institute, Carnegie Mellon University, February 2016. https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

[Cichonski 2012]
Cichonski, P., Millar, T., Grance, T., Scarfone, K. *Computer Security Incident Handling Guide*. National Institute of Standards and Technology Special Publication 800-61 Revision 2, August 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[Dempsey 2011]
Dempsey, K., Shah Chawla, N., Johnson, A., Johnston, R., Clay Jones, A., Orebaugh, A., Scholl, M., Stine, K. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. National Institute of Standards and Technology Special Publication 800-137, September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

[Grance 2006]
Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T. *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. National Institute of Standards and Technology Special Publication 800-84, September 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

[Jansen 2011]
Jansen, W., Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology Special Publication 800-144, December 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[Johnson 2011]
Johnson, A., Dempsey, K., Ross, R., Gupta, S., Bailey, D. *Guide for Security-Focused Configuration Management of Information Systems*. National Institute of Standards and Technology Special Publication 800-128, August 2011. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

[Kent 2006a]
Kent, K., Chevalier, S., Grance, T., Dang, H. *Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology Special Publication 800-86, August 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[Kent 2006b]
Kent, K., Souppaya, M. *Guide to Computer Security Log Management.* National Institute of Standards and Technology Special Publication 800-92, September 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[Newhouse 2017]
Newhouse, W., Keith, K., Scribner, B., Witte, G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology Special Publication 800-181, August 2017. https://csrc.nist.gov/pubs/sp/800/181/final
Superseded by [Petersen 2020].

[NIST 2004]
National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. FIPS Pub 199, February 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[NIST 2006]
National Institute of Standards and Technology. *Minimum Security Requirements for Federal Information and Information Systems*. FIPS Pub 200, March 2006. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[NIST 2012]
Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology Special Publication 800-30 Revision 1, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[NIST 2015]
Joint Task Force Transformation Initiative. *Security and Privacy Controls for Information Systems and Organizations* National Institute of Standards and Technology Special Publication 800-53 Revision 4, January 2015. https://csrc.nist.gov/pubs/sp/800/53/r4/upd3/final
Superseded by [NIST 2020].

[NIST 2018]
National Institute of Standards and Technology. *Cybersecurity Framework Version 1.1*, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[NIST 2020]
Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology Special Publication 800-53 Revision 5, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[Petersen 2020]
Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., Witte, G. *Workforce Framework for Cybersecurity (NICE Framework)*. National Institute of Standards and Technology Special Publication 800-181 Revision 1, November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[Quinn 2018]
Quinn, S., Souppaya, M., Cook, M., Scarfone, K. *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*. National Institute of Standards and Technology Special Publication 800-70 Revision 4, February 2018.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

[Scarfone 2008]
Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. *Technical Guide to Information Security Testing and Assessment.* National Institute of Standards and Technology Special Publication 800-115, September 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[Scarfone 2009]
Scarfone, K., Hoffman, P. *Guidelines on Firewalls and Firewall Policy*. National Institute of Standards and Technology Special Publication 800-41 Revision 1, September 2009.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[Souppaya 2022]
Souppaya, M., Scarfone, K. *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. National Institute of Standards and Technology Special Publication 800-40, Revision 4, April 2022.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-40r4.pdf

[Swanson 2006]
Swanson, M., Hash, J., Bowen, M. *Guide for Developing Security Plans for Federal Information Systems*. National Institute of Standards and Technology Special Publication 800-18, Revision 1, February 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[Swanson 2010]
Swanson, M., Bowen, M., Wohl Philips, A., Gallup, D., Lynes, D. *Contingency Planning Guide for Federal Information Systems*. National Institute of Standards and Technology Special Publication 800-34, Revision 1, May 2010.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[West-Brown 2003]
West-Brown, M., Stikvoort, D., Kossakowski, K-P., Killcrece, G., Ruefle, R., Zajicek, M. *Handbook for Computer Security Incident Response Teams (CSIRTs), Second Edition*. Software Engineering Institute, Carnegie Mellon University. April 2003.
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY