From: **Lauren Holloway** <LHolloway@pcisecuritystandards.org>
Date: Mon, Apr 10, 2017 at 7:11 PM
Subject: Cybersecurity Framework draft v1.1: comments
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Attached are my comments in the Excel version of the draft framework, to suggest that you add PCI DSS in the applicable rows of the Informative References column (I have already added them in the applicable rows in red).

Thank you and please let me know if you have any questions or comments.

Lauren Holloway
Director of Standards Coordination
CISSP, CISA, CISM
……
PCI Security Standards Council
Direct: +1-781-876-6284
Fax: +1-650-396-4343
Email: lholloway@pcisecuritystandards.org
Twitter: @PCISSC
Time Zone: Pacific (US & Canada)

draft-cybersecurity-fr
amework-v1.1-core-p

[Attachment Copied Below]

Function	Category	Subcategory	Informative References
IDENTIFY	**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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **PCI DSS v3.2** 2.4, 9.9, 11.1.1
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **PCI DSS v3.2** 2.4
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 • **PCI DSS v3.2** 1.1.2, 1.1.3
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9 • **PCI DSS v3.2** 8.1.5
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1

		• **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14 • **PCI DSS v3.2** 9.6.1, 12.2
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 • **PCI DSS v3.2** 12.4, 12.5, 12.8, 12.9
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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **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	• **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)	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental,	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1

and operational requirements are understood and inform the management of cybersecurity risk.		• **NIST SP 800-53 Rev. 4** -1 controls from all families • **PCI DSS v3.2** 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7 • **PCI DSS v3.2** 12.4, 12.5
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7 • **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1) • **PCI DSS v3.2** 3.1, 9.8, 12.10
	ID.GV-4: Governance and risk management processes address cybersecurity risks	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11 • **PCI DSS v3.2** 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1, 12.2
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	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • **PCI DSS v3.2** 6.1, 11.2, 11.3 12.2
	ID.RA-2: Cyber threat intelligence and vulnerability information is received	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4

	from information sharing forums and sources	• **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5 • **PCI DSS v3.2** 6.1
	ID.RA-3: Threats, both internal and external, are identified and documented	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16 • **PCI DSS v3.2** 6.1, 12.2
	ID.RA-4: Potential business impacts and likelihoods are identified	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14 • **PCI DSS v3.2** 6.1
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 • **PCI DSS v3.2** 12.2
	ID.RA-6: Risk responses are identified and prioritized	• **COBIT 5** APO12.05, APO13.02 • **NIST SP 800-53 Rev. 4** PM-4, PM-9 • **PCI DSS v3.2** 12.2, 12.10
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	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9 • **PCI DSS v3.2** 12.2
	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 • **NIST SP 800-53 Rev. 4** PM-9 • **PCI DSS v3.2** 12.2

	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14 • **PCI DSS v3.2** 12.2
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 in place 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:** 4.8 • **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:** SA-9, SA-12, PM-9 • **PCI DSS v3.2** 12.2, 12.8, 12.9
	ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process	• **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**: RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 • **PCI DSS v3.2** 12.2, 12.8
	ID.SC-3: Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	• **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:** SA-9, SA-11, SA-12, PM-9 • **PCI DSS v3.2** 12.8
	ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required.	• **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

		Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted	• **ISA 62443-3-3:2013:** SR 6.1 • **ISO/IEC 27001:2013:** A.15.2.1, A.15.2.2 • **NIST SP 800-53**: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 • **PCI DSS v3.2** 12.8
		ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers	• **CIS CSC:** 19.7, 20.3 • **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**: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management 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.	**PR.AC-1:** Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family • **PCI DSS v3.2** 8.1, 8.2, 12.3
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 • **PCI DSS v3.2** 9.1, 9.2, 9.3, 9.4, 9.5, 9.9, 9.10
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03

			• **ISA 62443-2-1:2009** 4.3.3.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20 • **PCI DSS v3.2** 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16 • **PCI DSS v3.2** 6.4.2, 7.1, 7.2
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7 • **PCI DSS v3.2** 1.1, 1.2, 2.2, 6.2, 10.8, 11.3
		PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	• **CIS CSC: CSC 5, 12, 14, 16** • **COBIT 5: DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03** • **ISA 62443-2-1:2009: 4.3.2.4.2, 4.3.3.2.2, 4.3.3.2.3, 4.3.3.5.2, 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 1.4, SR 1.5, SR 2.1, SR 2.2, SR 2.3** • **ISO/IEC 27001:2013: A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4** • **NIST SP 800-53: AC-2, AC-3, AC-5, AC-6, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3**

			• **PCI DSS v3.2** 7.1, 7.2, 8.1 (all), 8.2.2
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13 • **PCI DSS v3.2** 6.5, 9.9.3, 12.4, 12.6
		PR.AT-2: Privileged users understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13 • **PCI DSS v3.2** 1.1.5, 7.1 (all), 7.3, 12.4, 12.6
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9 • **PCI DSS v3.2** 2.6 (and Appendix A1 for hosting providers), 12.8, 12.9
		PR.AT-4: Senior executives understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13 • **PCI DSS v3.2** 12.5
			• **CCS CSC** 9 • **COBIT 5** APO07.03

		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• **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 • **PCI DSS v3.2** 12.5
	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.	**PR.DS-1:** Data-at-rest is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28 • **PCI DSS v3.2** 3.1, 3.3, 3.4, 3.5, 3.6, 3.7
		PR.DS-2: Data-in-transit is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8 • **PCI DSS v3.2** 4.1, 4.2, 4.3
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 • **PCI DSS v3.2** 2.4, 9.5, 9.6, 9.7, 9.8, 9.9, 11.1.1
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5

		PR.DS-5: Protections against data leaks are implemented	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7 • **PCI DSS v3.2** 10.5, 11.5
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2 • **PCI DSS v3.2** 6.4.1, 6.4.2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	• **CIS CSC: CSC 3.3** • **COBIT 5: BAI03.05.4** • **ISA 62443-2-1:2009: 4.3.4.4.4** • **ISA 62443-3-3:2013:** • **ISO/IEC 27001:2013: A.11.2.4** • **NIST SP 800-53: SA-10, SI-7**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6

	organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	security principles (e.g. concept of least functionality)	• **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 • **PCI DSS v3.2** 1.5, 2.2 (all), 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 • **PCI DSS v3.2** 6 (all)
		PR.IP-3: Configuration change control processes are in place	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 • **PCI DSS v3.2** 6.4 (all)
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 • **PCI DSS v3.2** 9.5.1, 12.10.1
		PR.IP-5: Policy and regulations regarding the physical operating	• **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

	environment for organizational assets are met	• **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 • **PCI DSS v3.2** 9 (all)
	PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6 • **PCI DSS v3.2** 3.1, 9.8
	PR.IP-7: Protection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 • **PCI DSS v3.2** 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8 • **PCI DSS v3.2** 11.1.2, 12.5.3, 12.10
	PR.IP-10: Response and recovery plans are tested	• **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

		• **PCI DSS v3.2** 12.10.2
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family • **PCI DSS v3.2** 8.1.3, 12.7
	PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 • **PCI DSS v3.2** 6.1, 6.2, 11.2
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5 • **PCI DSS v3.2** 6.2
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4 • **PCI DSS v3.2** 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9
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.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

		• **NIST SP 800-53 Rev. 4** AU Family • **PCI DSS v3.2** 10.1, 10.2, 10.3, 10.6.1, 10.6.2
	PR.PT-2: Removable media is protected and its use restricted according to policy	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7 • **PCI DSS v3.2** 3.4, 9.5
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7 • **PCI DSS v3.2** 2.2 (all), 7.1, 7.2, 9.3
	PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 • **PCI DSS v3.2** 1 (all), 2 (all), 4.1
	PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under	• **CIS CSC:** • **COBIT 5: BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05**

		attack, during recovery, normal operations).	• **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: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4 • **PCI DSS v3.2** 10.6.1, 11.4, 12.5.2
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • **PCI DSS v3.2** 10.1, 12.10.5
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4 • **PCI DSS v3.2** 12.5.2
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 • **PCI DSS v3.2** 12.5.2
	Security Continuous Monitoring (DE.CM): The information system	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07

	and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.		• **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 • **PCI DSS v3.2** 10.6.1, 11.4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• **ISA 62443-2-1:2009** 4.3.3.3.8 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 • **PCI DSS v3.2** 9.1.1
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • **PCI DSS v3.2** 9.1.1
		DE.CM-4: Malicious code is detected	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3 • **PCI DSS v3.2** 5 (all)
		DE.CM-5: Unauthorized mobile code is detected	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44 • **PCI DSS v3.2** 5 (all)
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 • **PCI DSS v3.2** 8.1.5
			• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• **PCI DSS v3.2** 10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5
		DE.CM-8: Vulnerability scans are performed	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5 • **PCI DSS v3.2** 11.2
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 • **PCI DSS v3.2** 12.5.2, 12.10
		DE.DP-2: Detection activities comply with all applicable requirements	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • **PCI DSS v3.2** 10.6.1, 10.9, 11.4, 11.5, 12.10
		DE.DP-4: Event detection information is communicated to appropriate parties	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4

			• **PCI DSS v3.2** 12.10
		DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 • **PCI DSS v3.2** 12.10
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 • **PCI DSS v3.2** 12.10
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 • **PCI DSS v3.2** 12.10
		RS.CO-2: Events are reported consistent with established criteria	• **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 • **PCI DSS v3.2** 12.10
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 • **PCI DSS v3.2** 12.10
			• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **PCI DSS v3.2** 12.10
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
		RS.AN-2: The impact of the incident is understood	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
		RS.AN-3: Forensics are performed	• **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 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
		RS.AN-4: Incidents are categorized consistent with response plans	• **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 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
	Mitigation (RS.MI): Activities are performed to prevent expansion of an	**RS.MI-1:** Incidents are contained	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4

	event, mitigate its effects, and eradicate the incident.		• **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
		RS.MI-2: Incidents are mitigated	• **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 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 • **PCI DSS v3.2** 10.6.3, 11.5.1, 12.5.2, 12.10
	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	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2** 12.10.6
		RS.IM-2: Response strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2** 12.10.6
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 • **PCI DSS v3.2** 12.10.6
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2** 12.10.6
			• **COBIT 5** BAI07.08

	RC.IM-2: Recovery strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 • **PCI DSS v3.2** 12.10.6
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• **COBIT 5** EDM03.02
	RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• **NIST SP 800-53 Rev. 4** CP-2, IR-4 • **PCI DSS v3.2** 12.10.6