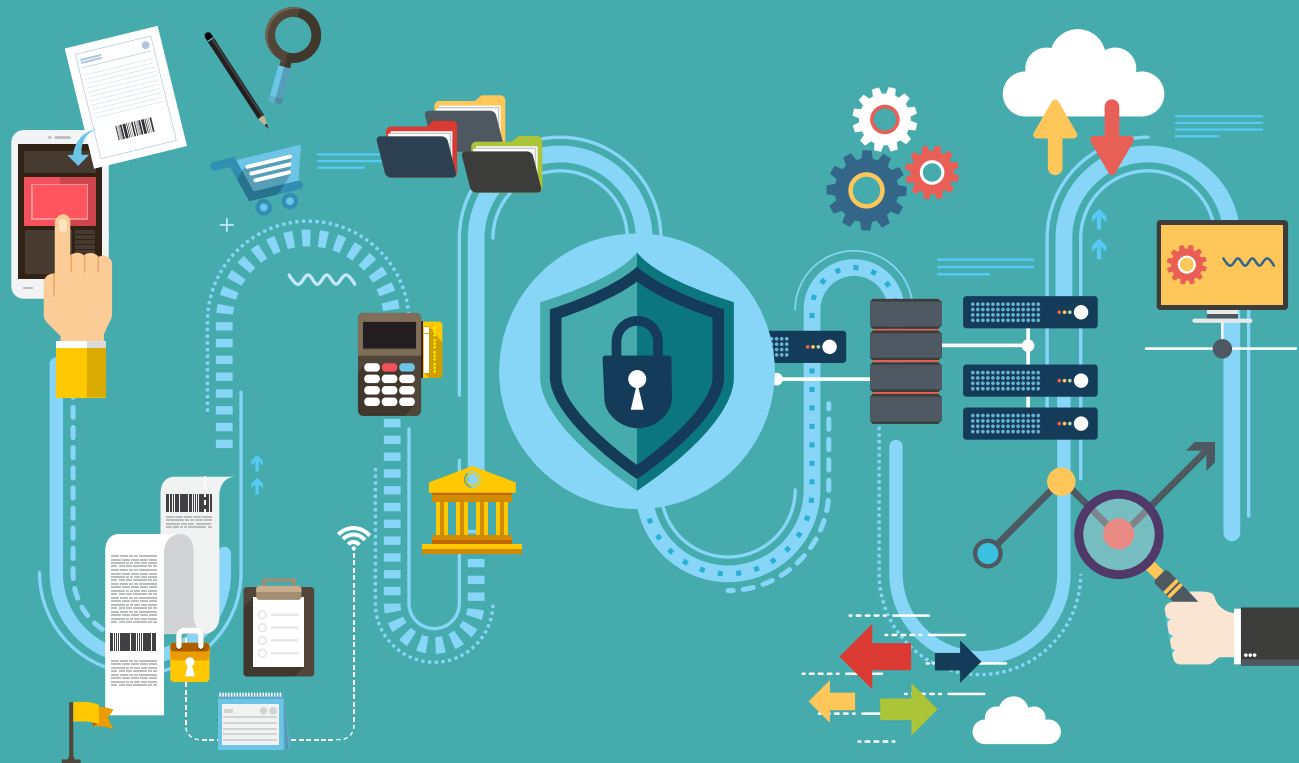


Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1

JULY 2019



Understanding the Mapping of PCI DSS to the NIST Cybersecurity Framework

The Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework ("the NIST Framework") share the common goal of enhancing data security. This document, created by the PCI Security Standards Council (PCI SSC), maps PCI DSS to the NIST Framework and provides a resource for stakeholders to use in understanding how to align security efforts to meet objectives in both PCI DSS and the NIST Framework.

PCI DSS is focused on the unique security threats and risks present in the payments industry. It defines security requirements for the protection of payment card data, as well as validation procedures and guidance to help organizations understand the intent of the requirements. PCI SSC works with merchants, service providers, financial institutions, technology vendors, and others in the payments industry, as well as our assessor and forensic investigator communities. This keeps all stakeholders aware of current risks to payment data and ensures that PCI Standards continue to address those risks.

The NIST Framework provides an overarching security and risk-management structure for voluntary use by U.S. critical infrastructure owners and operators. The NIST Framework core components consists of security Functions, Categories, and Subcategories of actions. These Subcategories reference globally recognized standards for cybersecurity. As the NIST Framework is broadly focused on organizational risk management, achieving the outcomes stated therein does not provide assurance that payment data is also protected.

Both PCI DSS and the NIST Framework are solid security approaches that address common security goals and principles as relevant to specific risks. While the NIST Framework identifies general security outcomes and activities, PCI DSS provides specific direction and guidance on how to meet security outcomes for payment environments. Because PCI DSS and the NIST Framework are intended for different audiences and uses, they are not interchangeable, and neither one is a replacement for the other.

Mapping PCI DSS to the NIST Framework

This mapping is based on PCI DSS v3.2.1 and the Cybersecurity Framework v1.1, using the 2018-04-16_framework_v.1.1_core" spreadsheet¹. PCI SSC evaluated each NIST Framework outcome (for example, ID.AM-1) against PCI DSS requirements and identified the relevant PCI DSS requirements for each outcome. The resultant mapping shows where the NIST Framework and PCI DSS contribute to the same security outcomes. PCI DSS requirements that map to an outcome are noted as "Informative References" in **blue** in the table below.

The mapping covers all NIST Framework Functions and Categories, with PCI DSS requirements directly mapping to 96 of the 108 Subcategories. The mapping illustrates how meeting PCI DSS requirements may help entities demonstrate how NIST Framework outcomes are achieved for payment environments.

¹ <https://www.nist.gov/cyberframework/framework>

How to Use this Mapping Document

Stakeholders can use this mapping to identify opportunities for control efficiencies and greater alignment between organizational security objectives. For example, the mapping can help identify where the implementation of a particular security control can support both a PCI DSS requirement and a NIST Framework outcome. Additionally, an entity's internal evaluations to determine the effectiveness of implemented controls may help the entity prepare for either a PCI DSS or NIST Framework assessment, or both. In this way, the mapping supports a consistent and coordinated approach to information security across an organization.

The mapping is not a tool for demonstrating compliance to either PCI DSS or the NIST Framework, nor does meeting either a PCI DSS requirement or its corresponding NIST Framework outcome result in the other being met.

Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1

This table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)"² other than the PCI DSS references in **blue**. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
FUNCTION: 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.	ID.AM-1: Physical devices and systems within the organization are inventoried.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 2.4, 9.9, 11.1.1, 12.3.3
	ID.AM-2: Software platforms and applications within the organization are inventoried.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 2.4, 12.3.7

² <https://www.nist.gov/cyberframework/framework>

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	ID.AM-3: Organizational communication and data flows are mapped.	<ul style="list-style-type: none"> • CIS CSC 12 • 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, A.13.2.2 • PCI DSS v3.2.1 1.1.2, 1.1.3
	ID.AM-4: External information systems are catalogued.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 1.1.1, 1.1.2, 1.1.3, 2.4
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.	<ul style="list-style-type: none"> • CIS CSC 13, 14 • COBIT 5 APO03.03, APO03.04, AP012.01, BA104.02, 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 • PCI DSS v3.2.1 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.	<ul style="list-style-type: none"> • CIS CSC 117, 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 • PCI DSS v3.2.1 12.4, 12.5, 12.8, 12.9

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • COBIT 5 APO08.01, AP008.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.1, A.15.1.12, 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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).	<ul style="list-style-type: none"> • OBIT 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

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • 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 families • PCI DSS v3.2.1 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: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	<ul style="list-style-type: none"> • 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 PM-1, PM-2, PS-7 • PCI DSS v3.2.1 12.4, 12.5, 12.8, 12.9
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	<ul style="list-style-type: none"> • CIS CSC 19 • COBIT 5 BJI02.01, 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 • PCI DSS v3.2.1 3.1, 12.10
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 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

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.1, 11.2, 11.3, 12.2
	ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources.	<ul style="list-style-type: none"> • 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 PM-15, PM-16, SI-5 • PCI DSS v3.2.1 6.1
	ID.RA-3: Threats, both internal and external, are identified and documented.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	ID.RA-4: Potential business impacts and likelihoods are identified.	<ul style="list-style-type: none"> • 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, PM-9, PM-11, SA-14 • PCI DSS v3.2.1 6.1
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.2
	ID.RA-6: Risk responses are identified and prioritized.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.1

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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	<ul style="list-style-type: none"> • CIS CSC 4 • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9 • PCI DSS v3.2.1 12.2
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 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	<ul style="list-style-type: none"> • COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 • NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 • PCI DSS v3.2.1 12.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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	<ul style="list-style-type: none"> • 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 v3.2.1 12.2, 12.8, 12.9
	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	<ul style="list-style-type: none"> • 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 v3.2.1 12.2, 12.8
	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 and Cyber Supply Chain Risk Management Plan.	<ul style="list-style-type: none"> • 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 v3.2.1 12.8, 12.9

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	<p>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.</p>	<ul style="list-style-type: none"> • 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: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 • PCI DSS v3.2.1 12.8
	<p>ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.</p>	<ul style="list-style-type: none"> • 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: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 • PCI DSS v3.2.1 12.10
FUNCTION: PROTECT (PR)		
<p>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.</p>	<p>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.</p>	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 2.1, 8.1, 8.2, 8.5, 8.6, 12.3

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.AC-2: Physical access to assets is managed and protected.	<ul style="list-style-type: none"> • 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.11.2.3 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 • PCI DSS v3.2.1 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.9, 9.10
	PR.AC-3: Remote access is managed.	<ul style="list-style-type: none"> • CIS CSC 12 • COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20 • PCI DSS v3.2.1 2.3, 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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.4.2, 7.1, 7.2, 8.7, 9.3

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	<p>PR.AC-5: Network integrity is protected (e.g. network segregations, network segmentation).</p>	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 1.1, 1.2, 1.3, 2.2, 6.2, 10.8, 11.3
	<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.</p>	<ul style="list-style-type: none"> • 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 1.3, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • ISO/IEC 27001:2013: A.7.1.1, A.9.1.2 • NIST SP 800-53: Rev 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 • PCI DSS v3.2.1 7.1.4, 8.1, 8.2.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	<p>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).</p>	<ul style="list-style-type: none"> • 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, • 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 • PCI DSS v3.2.1 8.2, 8.3
<p>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.</p>	<p>PR.AT-1: All users are informed and trained.</p>	<ul style="list-style-type: none"> • CIS CSC 17, 18 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 • NIST SP 800-53 Rev. 4 AT-2, PM-13 • PCI DSS v3.2.1 6.7, 7.3, 8.4, 9.9.3, 12.4, 12.6
	<p>PR.AT-2: Privileged users understand their roles and responsibilities.</p>	<ul style="list-style-type: none"> • CIS CSC 5, 17, 18 • COBIT 5 APO07.02, DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13 • PCI DSS v3.2.1 1.1.5, 7.1, 7.2, 7.3, 12.4, 12.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	<ul style="list-style-type: none"> • CIS CSC 17 • COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16 • PCI DSS v3.2.1 12.8.2, 12.9
	PR.AT-4: Senior executives understand their roles and responsibilities.	<ul style="list-style-type: none"> • CIS CSC 17, 19 • COBIT 5 EDM01.01, APO01.02, APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, PM-13 • PCI DSS v3.2.1 12.4, 12.5
	PR.AT-5: Physical cybersecurity security personnel understand their roles and responsibilities.	<ul style="list-style-type: none"> • CIS CSC 17 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13 • PCI DSS v3.2.1 12.4, 12.5

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • CIS CSC 13, 14 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 • PCI DSS v3.2.1 3 (all), 8.2.1
	PR.DS-2: Data-in-transit is protected.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 4 (all), 8.2.1
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 2.4, 9.5, 9.6, 9.7, 9.8, 9.9
	PR.DS-4: Adequate capacity to ensure availability is maintained.	<ul style="list-style-type: none"> • 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

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.DS-5: Protections against data leaks are implemented.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 11.5
	PR.DS-7: The development and testing environment(s) are separate from the production environment.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.4.1, 6.4.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	<ul style="list-style-type: none"> • 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: SA-10, SI-7 • PCI DSS v3.2.1 9.9.2
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.	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).	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 1.2, 2.2
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.3, 6.4, 6.5, 6.6, 6.7

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.IP-3: Configuration change control processes are in place.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.4
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 9.5.1, 12.10.1, 12.10.2
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 9 (all)

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.IP-6: Data is destroyed according to policy.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 3.1, 9.8
	PR.IP-7: Protection processes are improved.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.8, 12.10.6, 12.11
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • CIS CSC 19 • COBIT 5 APO12.06, DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 • NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 • PCI DSS v3.2.1 11.1.2, 12.5.3, 12.10

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	PR.IP-10: Response and recovery plans are tested.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.2
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	<ul style="list-style-type: none"> • CIS CSC 5, 16 • COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.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 • PCI DSS v3.2.1 8.1.3, 9.3, 12.7
	PR.IP-12: A vulnerability management plan is developed and implemented.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.1, 6.2, 6.5, 11.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	<ul style="list-style-type: none"> • COBIT 5 BAI03.10, BAI09.02, BAI09.0, 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 • PCI DSS v3.2.1 6.2, 9.9.3
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.1, 10.2, 10.3, 10.4, 10.5, 10.6.1, 10.6.2, 10.7
	PR.PT-2: Removable media is protected and its use restricted according to policy.	<ul style="list-style-type: none"> • 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.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 • PCI DSS v3.2.1 3.4, 9.5, 9.6, 9.7, 9.8, 12.3, 12.3.10

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	<p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p>	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 2.2, 7.1, 7.2, 9.3
	<p>PR.PT-4: Communications and control networks are protected.</p>	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 1 (all), 2 (all)
	<p>PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).</p>	<ul style="list-style-type: none"> • 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: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
FUNCTION: 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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 1.1.1, 1.1.2, 1.1.3
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.6 (all), 12.5.2
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.1, 12.10.5, 10.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	DE.AE-4: Impact of events is determined.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.6.3, 12.5.2
	DE.AE-5: Incident alert thresholds are established.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.5.2
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.	<ul style="list-style-type: none"> • CIS CSC 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 • PCI DSS v3.2.1 10.6.1, 10.6.2, 11.4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 9.1.1

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 9.1.1
	DE.CM-4: Malicious code is detected.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 5 (all)
	DE.CM-5: Unauthorized mobile code is detected.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 5 (all)
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 8.1.5, 10.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5
	DE.CM-8: Vulnerability scans are performed.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 11.2
	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	<ul style="list-style-type: none"> • 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 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 • PCI DSS v3.2.1 9.9.3, 12.5.2, 12.10
	DE.DP-2: Detection activities comply with all applicable requirements.	<ul style="list-style-type: none"> • 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, PM-14, SA-18, SI-4 • PCI DSS v3.2.1 10.9, 11.2, 11.3, 11.4, 12.10.1
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.		

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	DE.DP-3: Detection processes are tested.	<ul style="list-style-type: none"> • 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, A.7.2.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • PCI DSS v3.2.1 10.6.1, 10.9, 11.2, 11.3, 12.10
	DE.DP-4: Event detection information is communicated.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10
	DE.DP-5: Detection processes are continuously improved.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
FUNCTION: 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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10
	RS.CO-1: Personnel know their roles and order of operations when a response is needed.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2 12.10
	RS.CO-2: Incidents are reported consistent with established criteria.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.8, 12.10□□

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	RS.CO-3: Information is shared consistent with response plans.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	<ul style="list-style-type: none"> • CIS CSC 19 • COBIT 5 BAI08.04 • 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 • PCI DSS v3.2.1 12.10.1
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	<ul style="list-style-type: none"> • CIS CSC 19 • COBIT 5 BAI08.04 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
	RS.AN-2: The impact of the incident is understood.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 10.6.3, 11.5.1, 12.5.2
	RS.AN-3: Forensics are performed.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 11.5.1, 12.5.2
	RS.AN-4: Incidents are categorized consistent with response plans.	<ul style="list-style-type: none"> • CIS CSC 4, 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 • PCI DSS v3.2.1 11.5.1, 12.5.2
	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).	<ul style="list-style-type: none"> • CIS CSC 4, 19 • COBIT 5 EDM03.02, DSS05.07 • NIST 800-53 Rev 4 SI-5, PM-15 • PCI DSS v3.2.1 6.1, 6.2

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 11.5.1, 12.5.2
	RS.MI-2: Incidents are mitigated.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 11.5.1, 12.5.2
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 6.1, 6.2, 10.6.3, 11.2, 11.5.1, 12.5.2, 12.10
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and	RS.IM-1: Response plans incorporate lessons learned.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
previous detection/response activities.	RS.IM-2: Response strategies are updated.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.6
FUNCTION: 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 incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 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.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.6
	RC.IM-2: Recovery strategies are updated.	<ul style="list-style-type: none"> • 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 • PCI DSS v3.2.1 12.10.6

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES ³
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.	<ul style="list-style-type: none"> • COBIT 5 EDM03.02 • ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
	RC.CO-2: Reputation is repaired after an incident.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4

³ **Blue text** in this table has been added by PCI SSC and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcomes. *Only the blue text has been added.* All other content in this table is copied directly from the NIST Cybersecurity "Framework V1.1 Core (Excel)" at this URL: <https://www.nist.gov/cyberframework/framework>. PCI SSC is not responsible for the accuracy of the information from the NIST Framework, including the Informative References therefrom.