Mapping PCI DSS v4.0.1 to NIST CSF 2.0

JULY 2026

PCI Security Standards Council®

Introduction

This document, created by the PCI SSC Board of Advisors (BoA), is a mapping from the Payment Card Industry Data Security Standard v4.0.1 (PCI DSS) to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) 2.0.

PCI DSS v4.0.1 and NIST CSF 2.0 share the common goal of enhancing data security. The PCI DSS to NIST CSF 2.0 Mapping provides a tool for stakeholders to use in understanding how to align security efforts to meet objectives in both PCI DSS and NIST CSF.

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 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 CSF 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The NIST CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.

Meeting PCI DSS Requirements Can Help Toward Achieving NIST CSF Outcomes for Payment Environments

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

Mapping PCI DSS to NIST CSF

This mapping is based on PCI DSS v4.0.1 and NIST CSF 2.0. PCI SSC BoA participants evaluated each NIST CSF 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 NIST CSF and PCI DSS contribute to the same security outcomes.

The PCI DSS to NIST CSF mapping covers all Framework Functions and Categories, with PCI DSS requirements mapping to 103 of the 106 Subcategories. The mapping illustrates how meeting PCI DSS requirements can help toward achieving NIST CSF outcomes for payment environments.

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 CSF 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 CSF 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 NIST CSF, nor does meeting either a PCI DSS requirement or its corresponding NIST CSF category outcome result in the other being met.

Mapping PCI DSS v4.0.1 to NIST's Cybersecurity Framework (CSF) 2.0

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored		
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood	**GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management	12.1.1, 12.1.2, 12.1.3, 12.1.4
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	12.1.1, 12.1.4, 12.4.1, 12.5.2, 12.5.2.1, 12.8.1, 12.8.2, 12.8.5, 12.9.1, 12.9.2
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity – including privacy and civil liberties obligations – are understood and managed	3.2.1, 9.4.6, 9.4.7, 12.1.1, 12.1.2, 12.8.1, 12.8.2, 12.8.5, 12.9.1, 12.9.2
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	12.5.1, 12.5.2, 12.10.1
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	1.2.3, 1.2.4, 12.5.1, 12.5.2, 12.8.1, 12.8.4, 12.9.1, 12.9.2
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	**GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders	12.1.1, 12.1.2, 12.1.4
	GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	None
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	5.2.3.1, 5.3.2.1, 6.3.1, 6.3.3, 7.2.5.1, 8.6.3, 9.5.1.2.1, 10.4.2.1, 11.3.1.1, 11.6.1, 12.10.4.1, 12.3.3, 12.3.4, 12.5.3, 12.8.3
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	12.10.1, 12.10.2, 12.10.6

NIST CSF 2.0 Category		NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	12.5.3, 12.8.2, 12.8.4, 12.8.5, 12.9.1, 12.9.2, 12.10.1
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	5.2.3.1, 5.3.2.1, 6.3.1, 6.3.3, 7.2.5.1, 8.6.3, 9.5.1.2.1, 10.4.2.1, 11.3.1.1, 12.3.1, 12.3.2, 12.3.3, 12.3.4, 12.8.3, 12.10.4.1
		GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	None
	Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	**GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	6.2.2, 12.1.3, 12.1.4, 12.6.1, 12.10.6
		GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	1.1.2, 2.1.2, 3.1.2, 4.1.2, 5.1.2, 6.1.2, 7.1.2, 8.1.2, 9.1.2, 10.1.2, 11.1.2, 12.1.3
		GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	6.2.2, 12.1.4, 12.10.3
		GV.RR-04: Cybersecurity is included in human resources practices	7.2.2, 8.2.5, 9.3.1.1, 12.6.3, 12.7.1
	Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced	**GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	12.1.1, 12.1.2, 12.1.3, 12.1.4, 12.6.1
		GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	1.1.1, 2.1.1, 3.1.1, 4.1.1, 5.1.1, 6.1.1, 7.1.1, 8.1.1, 9.1.1, 10.1.1, 11.1.1, 12.1.2

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	**GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	10.7.1, 10.7.2, 12.10.2, 12.10.6, 12.3.1, 12.4.2, 12.4.2.1
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	10.7.1, 10.7.2, 11.4.4, 12.3.4, 12.4.2, 12.4.2.1, 12.5.2, 12.5.3, 12.8.4, 12.10.2, 12.10.6
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	7.2.5.1, 10.7.2, 11.3.1, 11.3.2, 11.4.4, 12.3.1, 12.3.4, 12.4.2
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	**GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	1.2.3, 1.2.4, 6.3.1, 6.3.2, 6.4.3, 12.1.4, 12.8.1, 12.8.3, 12.8.4, 12.8.5, 12.9.1, 12.9.2
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	12.1.4, 12.8.3, 12.8.4, 12.10.1
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	6.2.3, 6.3.1, 6.3.2, 6.4.3, 12.3.4, 12.8.3
	GV.SC-04: Suppliers are known and prioritized by criticality	1.2.4, 6.3.2, 12.5.2, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	12.8.1, 12.8.2, 12.8.3, 12.8.5, 12.9.1, 12.9.2
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	1.2.3, 1.2.4, 12.5.2, 12.8.1, 12.8.2, 12.8.3, 12.8.5

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	1.2.4, 6.3.1, 6.3.2, 6.4.3, 11.6.1, 12.5.2, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5, 12.9.1, 12.9.2
	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	1.2.3, 1.2.4, 12.8.1, 12.8.2, 12.8.5, 12.9.1, 12.10.1, 12.10.2, 12.10.5, 12.10.6
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	6.2.3, 6.3.1, 6.3.2, 6.3.3, 6.4.3, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 11.6.1, 12.3.4, 12.8.1, 12.8.4, 12.8.5
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	1.2.3, 1.2.4, 3.2.1, 6.4.3, 8.2.5, 9.3.1.1, 9.4.6, 9.4.7, 12.3.4, 12.5.2, 12.8.2, 12.8.3, 12.8.5, 12.10.1
IDENTIFY (ID): The organization's current cybersecurity risks are understood		
Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) 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-01:** Inventories of hardware managed by the organization are maintained	1.2.3, 9.5.1.1, 9.5.1.2, 12.5.1
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	6.3.2, 6.4.3, 12.5.1, 12.8.1
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	1.2.3, 1.2.4, 12.5.2
	ID.AM-04: Inventories of services provided by suppliers are maintained	12.8.1, 12.8.3, 12.8.4, 12.8.5
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	6.3.1, 9.5.1.2.1, 10.4.2.1, 12.3.1

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	3.2.1, 3.4.1, 3.4.2, 12.5.5, 12.10.7
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	6.2.1, 6.2.2, 6.2.3, 6.2.3.1, 6.2.4, 6.3.1, 6.3.3, 6.4.3, 12.3.4
Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	**ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded	6.3.1, 6.3.2, 11.3.1, 11.3.2
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	6.3.1
	ID.RA-03: Internal and external threats to the organization are identified and recorded	12.3.1
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	12.3.1
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	6.3.1, 6.3.3, 11.3.1.1, 12.3.1
	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	6.3.3, 11.3.1, 11.3.2, 12.10.1
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	8.6.3, 9.5.1.2.1, 10.4.2.1, 12.3.1, 12.3.2
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	6.3.1, 6.3.3
	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	6.4.3, 9.5.1.1
	ID.RA-10: Critical suppliers are assessed prior to acquisition	12.8.1, 12.8.2, 12.8.3

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all NIST CSF Functions	**ID.IM-01:** Improvements are identified from evaluations	12.3.1, 12.3.4, 12.4.2, 12.4.2.1
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	11.4.4, 12.8.4, 12.10.2, 12.10.6
	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	6.3.3, 10.7.1, 10.7.2, 11.3.1, 11.3.2, 11.4
	ID.IM-04: Incident response plans and other **c**ybersecurity plans that affect operations are established, communicated, maintained, and improved	12.10.1, 12.10.2, 12.10.3, 12.10.4, 12.10.6
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used		
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	**PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization	3.6.1.2, 3.6.1.3, 3.6.1.4, 8.2.1, 8.6.2, 8.6.3, 9.5.1.1
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	8.2.1, 8.3.5, 8.2.2, 12.7.1
	PR.AA-03: Users, services, and hardware are authenticated	2.2.2, 2.3.1, 3.5.1.3, 8.2.8, 8.3.1, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.3.10, 8.3.10.1, 8.4.1, 8.4.2, 8.4.3, 9.2.4
	PR.AA-04: Identity assertions are protected, conveyed, and verified	3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 4.2.1, 12.3.3
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	7.1.1, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.5.1, 7.2.6, 8.1.1, 8.2.6, 12.1.3
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	9.2.1, 9.2.2, 9.2.3, 9.3.1, 9.3.2, 9.3.3, 9.4.1, 9.2.4, 9.3.1.1, 9.5.1.2

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	**PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	12.6.1, 12.6.3
	PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	6.2.2, 12.10.4, 12.10.4.1
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected	3.3.1, 3.5.1, 3.5.1.3, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 9.4.6, 9.4.7
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	2.3.1, 4.2.1, 4.2.1.2, 12.3.3
	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	3.2.1, 3.4.1, 7.2.2, 8.2.8
	PR.DS-11: Backups of data are created, protected, maintained, and tested	9.3.1.1, 9.4.1.1, 9.4.7, 12.10.1
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-01:** Configuration management practices are established and applied	2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.3.1
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	6.2.4, 6.3.1, 6.3.2, 6.3.3, 12.3.4
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	9.4.7, 9.5.1.1, 12.3.4
	PR.PS-04: Log records are generated and made available for continuous monitoring	10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.4.2.1, 10.5.1, 10.6.1, 10.6.3
	PR.PS-05: Installation and execution of unauthorized software are prevented	2.2.1, 5.3.2, 6.4.3
	PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	6.2.2, 6.2.3, 6.3.2, 11.4.4

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage	1.2.3, 1.2.4, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1, 10.2.1, 11.2.1
	PR.IR-02: The organization's technology assets are protected from environmental threats	9.1.1, 9.2.1, 12.10.1
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	12.10.1, 12.10.2, 12.10.6
	PR.IR-04: Adequate resource capacity to ensure availability is maintained	None
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed		
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-01:** Networks and network services are monitored to find potentially adverse events	1.2.4, 10.2.1, 10.4.1, 11.2.1, 11.5.1
	DE.CM-02: The physical environment is monitored to find potentially adverse events	9.3.1.1, 9.4.1.2, 9.5.1.2
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	8.2.2, 10.2.1, 10.4.1, 10.6.1
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	7.2.4, 10.2.1, 11.6.1, 12.8.4
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	5.2.1, 5.2.2, 5.3.2, 6.4.3, 10.3.4, 11.3.1, 11.3.2, 11.6.1
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	**DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities	6.3.1, 10.2.1, 10.3.3, 10.3.4, 10.4.1, 10.4.2.1, 10.4.3, 10.7, 11.2.1, 12.10.5
	DE.AE-03: Information is correlated from multiple sources	1.2.4, 10.2.1, 10.3.3, 10.4.1, 10.4.2, 10.7, 12.5.1, 12.10.5
	DE.AE-04: The estimated impact and scope of adverse events are understood	1.2.3, 1.2.4, 10.2.1, 10.4.1, 10.4.2, 10.7, 12.5.1, 12.5.2, 12.5.2.1, 12.10.1

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
	DE.AE-06: Information on adverse events is provided to authorized staff and tools	10.3.1, 10.3.3, 12.10.1, 12.10.3
	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	6.3.1, 6.4.3, 12.3.4, 12.5.1, 12.10.6
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	12.10.1, 12.10.2, 12.10.4, 12.10.5
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken		
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	**RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared	12.8.2, 12.10.1, 12.10.2, 12.10.3
	RS.MA-02: Incident reports are triaged and validated	10.2.1, 10.4.1, 10.4.2, 10.4.3, 12.10.1, 12.10.4, 12.10.5
	RS.MA-03: Incidents are categorized and prioritized	10.4.1, 12.10.1, 12.10.4
	RS.MA-04: Incidents are escalated or elevated as needed	12.10.1, 12.10.2, 12.10.3
	RS.MA-05: The criteria for initiating incident recovery are applied	12.10.1, 12.10.2, 12.10.6
Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities	**RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident	6.3.1, 10.2.1, 10.2.2, 10.4.1, 12.10.1, 12.10.6
	RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.5.1, 10.6.1, 11.5.2
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	10.2.1, 10.2.2, 10.3.2, 10.3.3, 10.3.4, 10.5.1, 10.6.1
	RS.AN-08: An incident's magnitude is estimated and validated	1.2.3, 1.2.4, 10.4.1, 12.5.1

NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	PCI DSS v4.0.1 Requirement #
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**RS.CO-02:** Internal and external stakeholders are notified of incidents	12.8.2, 12.8.5, 12.10.1, 12.10.3
	RS.CO-03: Information is shared with designated internal and external stakeholders	12.8.2, 12.8.4, 12.10.1, 12.10.6
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-01:** Incidents are contained	5.2.1, 5.2.2, 5.3.2, 12.10.1
	RS.MI-02: Incidents are eradicated	2.2.1, 5.2.2, 6.2.3, 6.3.3, 12.10.1
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored		
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process	12.10.1, 12.10.2, 12.10.3
	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	1.2.3, 1.2.4, 12.10.1, 12.10.2, 12.10.6
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	5.3.2, 9.4.1.1, 9.4.1.2, 12.10.1
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	1.2.3, 1.2.4, 10.2.1, 12.5.1, 12.5.2, 12.10.1
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	6.2.3, 10.2.1, 10.4.1, 11.4.4, 11.5.1, 11.5.2
	RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	10.5.1, 12.10.2, 12.10.6
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	**RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	12.8.2, 12.8.4, 12.8.5, 12.10.1, 12.10.3
	RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	12.10.1, 12.10.3