NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: PCI DSS v4.0.1 - SAQ A
Focal Document URL: https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-pci-dss-4-0-1-saq-a.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.2.2	N/A	Vendor default accounts are managed as follows: ■ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ■ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	System components cannot be accessed using default passwords.
2.2.2	N/A	Vendor default accounts are managed as follows: ■ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ■ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	System components cannot be accessed using default passwords.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ■ Documented. ■ Kept up to date. ■ In use. ■ Known to all affected parties.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ■ Documented. ■ Kept up to date. ■ In use. ■ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ■ Documented. ■ Kept up to date. ■ In use. ■ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ■ Documented. ■ Kept up to date. ■ In use. ■ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.2.1	N/A	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: ■ Coverage for all locations of stored account data. ■ Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ■ Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. ■ Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. ■ Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. ■ A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.
3.2.1	N/A	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: ■ Coverage for all locations of stored account data. ■ Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ■ Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. ■ Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. ■ Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. ■ A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ■ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ■ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ■ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ■ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ■ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ■ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ■ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ■ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ■ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ■ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ■ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ■ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.4.3	N/A	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: ■ A method is implemented to confirm that each script is authorized. ■ A method is implemented to assure the integrity of each script. ■ An inventory of all scripts is maintained with written justification as to why each is necessary.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.
6.4.3	N/A	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: ■ A method is implemented to confirm that each script is authorized. ■ A method is implemented to assure the integrity of each script. ■ An inventory of all scripts is maintained with written justification as to why each is necessary.	Functional	Intersects With	Unauthorized Code	WEB-01.1	Mechanisms exist to prevent unauthorized code from being present in a secure page as it is rendered in a client's browser.	5	Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.
8.2.1	N/A	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	All actions by all users are attributable to an individual.
8.2.1	N/A	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	All actions by all users are attributable to an individual.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ■ Account use is prevented unless needed for an exceptional circumstance. ■ Use is limited to the time needed for the exceptional circumstance. ■ Business justification for use is documented. ■ Use is explicitly approved by management. ■ Individual user identity is confirmed before access to an account is granted. ■ Every action taken is attributable to an individual user.	Functional	Intersects With	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ■ Account use is prevented unless needed for an exceptional circumstance. ■ Use is limited to the time needed for the exceptional circumstance. ■ Business justification for use is documented. ■ Use is explicitly approved by management. ■ Individual user identity is confirmed before access to an account is granted. ■ Every action taken is attributable to an individual user.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ■ Account use is prevented unless needed for an exceptional circumstance. ■ Use is limited to the time needed for the exceptional circumstance. ■ Business justification for use is documented. ■ Use is explicitly approved by management. ■ Individual user identity is confirmed before access to an account is granted. ■ Every action taken is attributable to an individual user.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	5	The accounts of terminated users cannot be used.
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.5	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.6	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: ■ A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). ■ Contain both numeric and alphabetic characters.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A guessed password/passphrase cannot be verified by either an online or offline brute force attack.
8.3.7	N/A	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.7	N/A	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.9	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.3.9	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An undetected compromised password/passphrase cannot be used indefinitely.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.3.9	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An undetected compromised password/passphrase cannot be used indefinitely.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	Media are classified and protected appropriately.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	Media are classified and protected appropriately.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ■ Media sent outside the facility is logged. ■ Media is sent by secured courier or other delivery method that can be accurately tracked. ■ Offsite tracking logs include details about media location.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	Media is secured and tracked when transported outside the facility.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ■ Media sent outside the facility is logged. ■ Media is sent by secured courier or other delivery method that can be accurately tracked. ■ Offsite tracking logs include details about media location.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	Media is secured and tracked when transported outside the facility.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive/regulated media that is transferred outside of the organization's facilities.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
11.3.2	N/A	External vulnerability scans are performed as follows: ■ At least once every three months. ■ By a PCI SSC Approved Scanning Vendor (ASV). ■ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ■ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ■ At least once every three months. ■ By a PCI SSC Approved Scanning Vendor (ASV). ■ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ■ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ■ At least once every three months. ■ By a PCI SSC Approved Scanning Vendor (ASV). ■ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ■ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ■ At least once every three months. ■ By a PCI SSC Approved Scanning Vendor (ASV). ■ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ■ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	This requirement is not eligible for the customized approach.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ■ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ■ Rescans are conducted as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ■ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ■ Rescans are conducted as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ■ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ■ Rescans are conducted as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ■ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ■ Rescans are conducted as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ■ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ■ Rescans are conducted as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ■ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ■ The mechanism is configured to evaluate the received HTTP header and payment page. ■ The mechanism functions are performed as follows: - At least once every seven days OR - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ■ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ■ The mechanism is configured to evaluate the received HTTP header and payment page. ■ The mechanism functions are performed as follows: - At least once every seven days OR - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Website Change Detection	WEB-13	Mechanisms exist to detect and respond to Indicators of Compromise (IoC) for unauthorized alterations, additions, deletions or changes on websites that store, process and/or transmit sensitive/regulated data.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:(1) Contractual obligations for the External Service Provider (ESP);(2) Business practices;(3) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	Records are maintained of TPSPs and the services provided.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.3	N/A	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.
12.8.4	N/A	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	The PCI DSS compliance status of TPSPs is verified periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	A comprehensive incident response plan that meets card brand expectations is maintained.