

## NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Secure Controls Framework (SCF) version 2026.1  
<https://securecontrolsframework.com/set-theory-relationship-mapping-strm/>

Focal Document:  
 Focal Document URL:  
 Published STRM URL:

PCI DSS v4.0.1 - SAO B  
[https://east.pcisecuritystandards.org/document\\_library/category=pcids4&document=pci\\_dss\\_v4\\_0\\_1\\_sao\\_b.pdf](https://east.pcisecuritystandards.org/document_library/category=pcids4&document=pci_dss_v4_0_1_sao_b.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
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: <ul style="list-style-type: none"> <li>Documented.</li> <li>Kept up to date.</li> <li>In use.</li> <li>Known to all affected parties.</li> </ul>	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: <ul style="list-style-type: none"> <li>Documented.</li> <li>Kept up to date.</li> <li>In use.</li> <li>Known to all affected parties.</li> </ul>	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: <ul style="list-style-type: none"> <li>Documented.</li> <li>Kept up to date.</li> <li>In use.</li> <li>Known to all affected parties.</li> </ul>	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: <ul style="list-style-type: none"> <li>Documented.</li> <li>Kept up to date.</li> <li>In use.</li> <li>Known to all affected parties.</li> </ul>	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.
3.3.1	N/A	SAO is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.1	N/A	The full contents of any track are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.2	N/A	The card verification code is not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.3	N/A	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> <li>job classification and function.</li> <li>Least privileges necessary to perform job responsibilities.</li> </ul>	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> <li>job classification and function.</li> <li>Least privileges necessary to perform job responsibilities.</li> </ul>	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> <li>job classification and function.</li> <li>Least privileges necessary to perform job responsibilities.</li> </ul>	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> <li>job classification and function.</li> <li>Least privileges necessary to perform job responsibilities.</li> </ul>	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
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: <ul style="list-style-type: none"> <li>Media sent outside the facility is logged.</li> <li>Media is sent by secured courier or other delivery method that can be accurately tracked.</li> <li>Offline tracking logs include details about media location.</li> </ul>	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: <ul style="list-style-type: none"> <li>Media sent outside the facility is logged.</li> <li>Media is sent by secured courier or other delivery method that can be accurately tracked.</li> <li>Offline tracking logs include details about media location.</li> </ul>	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: <ul style="list-style-type: none"> <li>Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.</li> <li>Materials are stored in secure storage containers prior to destruction.</li> </ul>	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 purposes 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: <ul style="list-style-type: none"> <li>Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.</li> <li>Materials are stored in secure storage containers prior to destruction.</li> </ul>	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: <ul style="list-style-type: none"> <li>Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.</li> <li>Materials are stored in secure storage containers prior to destruction.</li> </ul>	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.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> <li>Maintaining a list of POI devices.</li> <li>Periodically inspecting POI devices to look for tampering or unauthorized substitution.</li> <li>Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.</li> </ul>	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> <li>Maintaining a list of POI devices.</li> <li>Periodically inspecting POI devices to look for tampering or unauthorized substitution.</li> <li>Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.</li> </ul>	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> <li>Maintaining a list of POI devices.</li> <li>Periodically inspecting POI devices to look for tampering or unauthorized substitution.</li> <li>Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.</li> </ul>	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> <li>Maintaining a list of POI devices.</li> <li>Periodically inspecting POI devices to look for tampering or unauthorized substitution.</li> <li>Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.</li> </ul>	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.

FDE #	FDE Name	Focal Document Element (FDE) Descriptions	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or modifications.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ■ Make and model of the device. ■ Location of device. ■ Device serial number or other methods of unique identification.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The identity and location of POI devices is recorded and known at all times.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ■ Make and model of the device. ■ Location of device. ■ Device serial number or other methods of unique identification.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	The identity and location of POI devices is recorded and known at all times.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ■ Make and model of the device. ■ Location of device. ■ Device serial number or other methods of unique identification.	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The identity and location of POI devices is recorded and known at all times.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ■ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ■ Procedures to ensure devices are not installed, replaced, or returned without verification. ■ Being aware of suspicious behavior around devices. ■ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ■ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ■ Procedures to ensure devices are not installed, replaced, or returned without verification. ■ Being aware of suspicious behavior around devices. ■ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ■ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ■ Procedures to ensure devices are not installed, replaced, or returned without verification. ■ Being aware of suspicious behavior around devices. ■ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ■ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ■ Procedures to ensure devices are not installed, replaced, or returned without verification. ■ Being aware of suspicious behavior around devices. ■ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ■ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ■ Procedures to ensure devices are not installed, replaced, or returned without verification. ■ Being aware of suspicious behavior around devices. ■ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
12.1.1	N/A	An overall information security policy is: ■ Established. ■ Published. ■ Maintained. ■ Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	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	The strategic objectives and principles of information security are defined, adopted, and known to all personnel.
12.1.1	N/A	An overall information security policy is: ■ Established. ■ Published. ■ Maintained. ■ Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	The strategic objectives and principles of information security are defined, adopted, and known to all personnel.
12.1.2	N/A	The information security policy is: ■ Reviewed at least once every 12 months. ■ Updated as needed to reflect changes to business objectives or risks to the environment.	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	The information security policy continues to reflect the organization's strategic objectives and principles.
12.1.2	N/A	The information security policy is: ■ Reviewed at least once every 12 months. ■ Updated as needed to reflect changes to business objectives or risks to the environment.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	The information security policy continues to reflect the organization's strategic objectives and principles.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	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	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRCP).	5	Personnel understand their role in protecting the entity's cardholder data.

FDE #	FDE Name	Focal Document Element (FDE) Descriptions	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	Personnel understand their role in protecting the entity's cardholder data.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific trainings.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
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 (RASC) 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 TPSP possesses 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 (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) 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 TPSP possesses 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 TPSP possesses 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 (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) 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.