

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

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

Focal Document:
 Focal Document URL:
 Published STRM URL:

PCI DSS v4.0.1 - SAO CVT
https://east.pcisecuritystandards.org/document_library?category=pcids&document=pci_dss_v4_0_1_sao_cv1.pdf
<https://content.securecontrolsframework.com/strm/pci-dss-4-0-1-sao-cv1.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 |
|-------|----------|---|----------------|-------------------|--|----------|---|--------------------------|---|
| 1.3.1 | N/A | Inbound traffic to the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Data Flow Enforcement - Access Control Lists (ACLs) | NET-04 | Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized. | 5 | Unauthorized traffic cannot enter the CDE. |
| 1.3.1 | N/A | Inbound traffic to the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Deny Traffic by Default & Allow Traffic by Exception | NET-04.1 | Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). | 5 | Unauthorized traffic cannot enter the CDE. |
| 1.3.1 | N/A | Inbound traffic to the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Network Segmentation (macrosegmentation) | NET-06 | Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources. | 5 | Unauthorized traffic cannot enter the CDE. |
| 1.3.1 | N/A | Inbound traffic to the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | DMZ Networks | NET-08.1 | Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks. | 5 | Unauthorized traffic cannot enter the CDE. |
| 1.3.2 | N/A | Outbound traffic from the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Prevent Unauthorized Exfiltration | NET-03.5 | Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive regulated data across managed interfaces. | 5 | Unauthorized traffic cannot leave the CDE. |
| 1.3.2 | N/A | Outbound traffic from the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Data Flow Enforcement - Access Control Lists (ACLs) | NET-04 | Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized. | 5 | Unauthorized traffic cannot leave the CDE. |
| 1.3.2 | N/A | Outbound traffic from the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Deny Traffic by Default & Allow Traffic by Exception | NET-04.1 | Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). | 5 | Unauthorized traffic cannot leave the CDE. |
| 1.3.2 | N/A | Outbound traffic from the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | Network Segmentation (macrosegmentation) | NET-06 | Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources. | 5 | Unauthorized traffic cannot leave the CDE. |
| 1.3.2 | N/A | Outbound traffic from the CDE is restricted as follows: ■ To only traffic that is necessary. ■ All other traffic is specifically denied. | Functional | Intersects With | DMZ Networks | NET-08.1 | Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks. | 5 | Unauthorized traffic cannot leave the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Guest Networks | NET-02.2 | Mechanisms exist to implement and manage a secure guest network. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Boundary Protection | NET-03 | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Isolation of System Components | NET-03.7 | Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Deny Traffic by Default & Allow Traffic by Exception | NET-04.1 | Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Policy Decision Point (PDP) | NET-04.7 | Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | Network Segmentation (macrosegmentation) | NET-06 | Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | Functional | Intersects With | DMZ Networks | NET-08.1 | Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks. | 5 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.3.3 | N/A | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ■ All wireless traffic from wireless networks into the CDE is denied by default. ■ Only wireless traffic with an authorized business purpose is allowed into the CDE. | 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 | Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Intersects With | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations. | 5 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Intersects With | Split Tunneling | CFG-03.4 | Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards. | 5 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Intersects With | Limits of Authorized Use | DCH-13.1 | Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individually first:(1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS. | 5 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Subset Of | Endpoint Device Management (EDM) | END-01 | Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls. | 10 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Intersects With | Endpoint Protection Measures | END-02 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 5 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 1.5.1 | N/A | Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ■ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ■ Security controls are actively running. ■ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | Functional | Intersects With | Software Firewall | END-05 | Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible. | 5 | Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE. |
| 2.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 2 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 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 2.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 2 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 (SCR), 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 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 2.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 2 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 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 2.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 2 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 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |

| 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 | IAE-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. |
| 2.2.4 | N/A | Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality 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 compromised by exploiting unnecessary functionality present in the system component. |
| 2.2.4 | N/A | Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. | Functional | Intersects With | Least Functionality | CFG-03 | Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services. | 5 | System components cannot be compromised by exploiting unnecessary functionality present in the system component. |
| 2.2.4 | N/A | Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. | Functional | Intersects With | Compensating Countermeasures | RSK-06.2 | Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats. | 5 | System components cannot be compromised by exploiting unnecessary functionality present in the system component. |
| 2.2.5 | N/A | If any insecure services, protocols, or daemons are present: ■ Business justification is documented. ■ Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. | 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 compromised by exploiting insecure services, protocols, or daemons. |
| 2.2.5 | N/A | If any insecure services, protocols, or daemons are present: ■ Business justification is documented. ■ Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. | Functional | Intersects With | Insecure Ports, Protocols & Services | TDA-02.6 | Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate cryptographic solutions. | 5 | System components cannot be compromised by exploiting insecure services, protocols, or daemons. |
| 2.2.6 | N/A | System security parameters are configured to prevent misuse. | Functional | Intersects With | Physical Diagnostic & Test Interfaces | TDA-05.1 | Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse. | 5 | System components cannot be compromised because of incorrect security parameter configuration. |
| 2.2.7 | N/A | All non-console administrative access is encrypted using strong cryptography. | Functional | Subset Of | Use of Cryptographic Controls | CRY-01 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 10 | Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions. |
| 2.2.7 | N/A | All non-console administrative access is encrypted using strong cryptography. | Functional | Intersects With | Automated Authentication Through Cryptographic Modules | CRY-02 | Automated mechanisms exist to enable systems to authenticate to a cryptographic module. | 5 | Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions. |
| 2.2.7 | N/A | All non-console administrative access is encrypted using strong cryptography. | Functional | Intersects With | Non-Console Administrative Access | CRY-06 | Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access. | 5 | Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions. |
| 2.2.7 | N/A | All non-console administrative access is encrypted using strong cryptography. | Functional | Intersects With | Remote Maintenance Cryptographic Protection | MMT-05.3 | Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications. | 5 | Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions. |
| 2.3.1 | N/A | For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ■ Default wireless encryption keys. ■ Passwords on wireless access points. ■ SNMP defaults. ■ Any other security-related wireless vendor defaults. | Functional | Intersects With | Wireless Access Authentication & Encryption | CRY-07 | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption. | 5 | Wireless networks cannot be accessed using vendor default passwords or default configurations. |
| 2.3.1 | N/A | For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ■ Default wireless encryption keys. ■ Passwords on wireless access points. ■ SNMP defaults. ■ Any other security-related wireless vendor defaults. | Functional | Intersects With | Default Authenticators | IAE-10.8 | Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation. | 5 | Wireless networks cannot be accessed using vendor default passwords or default configurations. |
| 2.3.1 | N/A | For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ■ Default wireless encryption keys. ■ Passwords on wireless access points. ■ SNMP defaults. ■ Any other security-related wireless vendor defaults. | 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 | Wireless networks cannot be accessed using vendor default passwords or default configurations. |
| 2.3.1 | N/A | For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ■ Default wireless encryption keys. ■ Passwords on wireless access points. ■ SNMP defaults. ■ Any other security-related wireless vendor defaults. | Functional | Intersects With | Authentication & Encryption | NET-15.1 | Mechanisms exist to secure WiFi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and(2) Encrypting transmitted data. | 5 | Wireless networks cannot be accessed using vendor default passwords or default configurations. |
| 2.3.2 | N/A | For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ■ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ■ Whenever a key is suspected of or known to be compromised. | Functional | Intersects With | Wireless Access Authentication & Encryption | CRY-07 | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption. | 5 | Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks. |
| 2.3.2 | N/A | For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ■ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ■ Whenever a key is suspected of or known to be compromised. | Functional | Intersects With | Cryptographic Key Loss or Change | CRY-03 | Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users. | 5 | Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks. |
| 2.3.2 | N/A | For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ■ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ■ Whenever a key is suspected of or known to be compromised. | 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 | Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks. |
| 2.3.2 | N/A | For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ■ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ■ Whenever a key is suspected of or known to be compromised. | Functional | Intersects With | Authentication & Encryption | NET-15.1 | Mechanisms exist to secure WiFi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and(2) Encrypting transmitted data. | 5 | Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks. |
| 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 (SCRPR), 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. |
| 3.3.1 | N/A | SAD 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. |
| 3.3.1.2 | 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. |
| 3.4.1 | 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/regulate 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 | PR-05.3 | Mechanisms exist to mask sensitive/regulate 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. |
| 4.2.1.2 | N/A | Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission. | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data transmissions. | 5 | Cleartext PAN cannot be read or intercepted from wireless network transmissions. |
| 4.2.1.2 | N/A | Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission. | Functional | Intersects With | Wireless Access Authentication & Encryption | CRY-07 | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption. | 5 | Cleartext PAN cannot be read or intercepted from wireless network transmissions. |
| 4.2.1.2 | N/A | Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission. | 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 | Cleartext PAN cannot be read or intercepted from wireless network transmissions. |
| 5.2.1 | N/A | An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware. |
| 5.2.2 | N/A | The deployed anti-malware solution(s): ■ Detects all known types of malware. ■ Removes, blocks, or contains all known types of malware. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Malware cannot execute or infect other system components. |
| 5.3.1 | N/A | The anti-malware solution(s) is kept current via automatic updates. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Anti-malware mechanisms can detect and address the latest malware threats. |
| 5.3.1 | N/A | The anti-malware solution(s) is kept current via automatic updates. | Functional | Intersects With | Automatic Antimalware Signature Updates | END-04.1 | Automated mechanisms exist to update anti-malware technologies, including signature definitions. | 5 | Anti-malware mechanisms can detect and address the latest malware threats. |
| 5.3.2 | N/A | The anti-malware solution(s): ■ Performs periodic scans and active or real-time scans. OR ■ Performs continuous behavioral analysis of systems or processes. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Malware cannot complete execution. |
| 5.3.2 | N/A | The anti-malware solution(s): ■ Performs periodic scans and active or real-time scans. OR ■ Performs continuous behavioral analysis of systems or processes. | Functional | Intersects With | Always On Protection | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period. | 5 | Malware cannot complete execution. |

| 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 |
|-------|----------|--|----------------|-------------------|---|----------|---|--------------------------|--|
| 5.3.3 | N/A | For removable electronic media, the anti-malware solution(s): <ul style="list-style-type: none"> Performs automatic scans of when the media is inserted, connected, or logically mounted. Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Malware cannot be introduced to system components via external removable media. |
| 5.3.3 | N/A | For removable electronic media, the anti-malware solution(s): <ul style="list-style-type: none"> Performs automatic scans of when the media is inserted, connected, or logically mounted. Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. | Functional | Intersects With | Always On Protection | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period. | 5 | Malware cannot be introduced to system components via external removable media. |
| 5.3.4 | N/A | Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Historical records of anti-malware actions are immediately available and retained for at least 12 months. |
| 5.3.4 | N/A | Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. | Functional | Intersects With | Centralized Management of Antimalware Technologies | END-04.3 | Mechanisms exist to centrally-manage anti-malware technologies. | 5 | Historical records of anti-malware actions are immediately available and retained for at least 12 months. |
| 5.3.5 | N/A | Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code. | 5 | Anti-malware mechanisms cannot be modified by unauthorized personnel. |
| 5.3.5 | N/A | Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. | Functional | Intersects With | Always On Protection | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period. | 5 | Anti-malware mechanisms cannot be modified by unauthorized personnel. |
| 5.4.1 | N/A | Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. | Functional | Intersects With | Phishing & Spam Protection | END-08 | Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail. | 5 | Mechanisms are in place to protect against and mitigate risk posed by phishing attacks. |
| 6.3.1 | N/A | Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> 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 & Flow Remediation During Development | IAD-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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 & Flow 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: <ul style="list-style-type: none"> 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 (VPM) | 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. |
| 6.3.1 | N/A | Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> 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 Flow Remediation Processes | VPM-05.1 | Mechanisms exist to centrally-manage the flow 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: <ul style="list-style-type: none"> 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 (VPM) | 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. |

| 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 |
|-------|----------|--|----------------|-------------------|---|----------|---|--------------------------|---|
| 6.3.3 | N/A | All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: <ul style="list-style-type: none"> Critical or high-severity 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 | VRM-05.1 | Mechanisms exist to centrally-manage the flaw remediation process. | 5 | System components cannot be compromised via the exploitation of a known vulnerability. |
| 7.2.2 | N/A | Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> Job classification and function. Least privileges necessary to perform job responsibilities. | 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"> Job classification and function. Least privileges necessary to perform job responsibilities. | 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"> Job classification and function. Least privileges necessary to perform job responsibilities. | 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"> Job classification and function. Least privileges necessary to perform job responsibilities. | 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. |
| 8.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 8 are: <ul style="list-style-type: none"> 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 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 8.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 8 are: <ul style="list-style-type: none"> 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 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 8.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 8 are: <ul style="list-style-type: none"> 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 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 8.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 8 are: <ul style="list-style-type: none"> 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 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. |
| 8.2.4 | N/A | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. | 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 | Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization. |
| 8.2.4 | N/A | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. | 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 | Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization. |
| 8.2.4 | N/A | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. | 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 | Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization. |
| 8.2.4 | N/A | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. | 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 | Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization. |
| 8.2.4 | N/A | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. | Functional | Intersects With | Account Management | IAC-15 | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts. | 5 | Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization. |
| 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. |
| 8.3.6 | N/A | If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: <ul style="list-style-type: none"> 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. |
| 8.4.1 | N/A | MFA is implemented for all non-console access into the CDE for personnel with administrative access. | Functional | Intersects With | Network Access to Privileged Accounts | IAC-06.1 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts. | 5 | Administrative access to the CDE cannot be obtained by the use of a single authentication factor. |
| 9.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> 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 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 9.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> 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 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 9.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> 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 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |

| 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 |
|----------|----------|---|----------------|-------------------|---|----------|--|--------------------------|---|
| 9.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 9 are: ■ Documented. ■ Kept 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 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 9.1.1 | N/A | All security policies and operational procedures that are identified in Requirement 9 are: ■ Documented. ■ Kept to date. ■ In use. ■ Known to all affected parties. | Functional | Subset Of | Physical & Environmental Protections | PES-01 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 10 | Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent. |
| 9.2.1 | N/A | Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | Functional | Intersects With | Physical Access Authorizations | PE-02 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 5 | System components in the CDE cannot be physically accessed by unauthorized personnel. |
| 9.2.1 | N/A | Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | Functional | Intersects With | Role-Based Physical Access | PE-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual. | 5 | System components in the CDE cannot be physically accessed by unauthorized personnel. |
| 9.2.1 | N/A | Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | Functional | Intersects With | Physical Access Control | PE-03 | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5 | System components in the CDE cannot be physically accessed by unauthorized personnel. |
| 9.2.1 | N/A | Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | Functional | Intersects With | Controlled Ingress & Egress Points | PE-03.1 | Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points. | 5 | System components in the CDE cannot be physically accessed by unauthorized personnel. |
| 9.2.1 | N/A | Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | Functional | Intersects With | Physical Access Logs | PE-03.3 | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points. | 5 | System components in the CDE cannot be physically accessed by unauthorized personnel. |
| 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 | PRJ-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 records, assets, and/or anonymize 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. |
| 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 (SCRP), 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 (SCRP), 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. |
| 12.6.1 | 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 training. | 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. |
| 12.6.3.1 | N/A | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ■ Phishing and related attacks. ■ Social engineering. | 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 their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required. |
| 12.6.3.1 | N/A | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ■ Phishing and related attacks. ■ Social engineering. | Functional | Intersects With | Social Engineering & Mining | SAT-02.2 | Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining. | 5 | Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required. |
| 12.6.3.1 | N/A | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ■ Phishing and related attacks. ■ Social engineering. | 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 their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required. |
| 12.6.3.1 | N/A | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ■ Phishing and related attacks. ■ Social engineering. | 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 their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required. |
| 12.6.3.1 | N/A | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ■ Phishing and related attacks. ■ Social engineering. | 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 their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel 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. |

| 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 |
|---------|----------|---|----------------|-------------------|--|----------|--|--------------------------|--|
| | | | | | | | | | |
| 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 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 (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 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 (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 verifying 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. |