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

Focal Document: **PCI DSS v4.0.1 - SAQ B-IP**
Focal Document URL: https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-pci-dss-4-0-1-saq-b-ip.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
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	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	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	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	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	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 representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	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	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	Network Segmentation (macrosegementation)	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 network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	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 network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	Identification & Justification of Ports, Protocols & Services	TDA-02.5	Mechanisms exist to require process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services (TAAS).	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	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 technology solutions.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Network Segmentation (macrosegementation)	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	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	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	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	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	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
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 (macrosegementation)	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 (macrosegementation)	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 (macrosegementation)	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.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ■ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ■ Stateful responses to communications initiated by system components in a trusted network. ■ All other traffic is denied.	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	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	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	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS) Deployment	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments.	5	Packets with forged IP source addresses cannot enter a trusted network.
2.2.2	N/A	Vendor default accounts are managed as follows: ■ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ■ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	System components cannot be accessed using default passwords.
2.2.2	N/A	Vendor default accounts are managed as follows: ■ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ■ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	System components cannot be accessed using default passwords.

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
2.2.7	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	MNT-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	IAC-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 Wi-Fi (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-09.3	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 Wi-Fi (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 (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.3.1	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.
3.3.1.1	N/A	The full contents of any track are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.2	N/A	The card verification code is not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.3	N/A	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	System components cannot be compromised via the exploitation of a known vulnerability.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: ▪ 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: ▪ 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: ▪ 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: ▪ 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: ▪ 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: ▪ 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: ▪ 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: ▪ 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.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ■ Enabled only during the time period needed and disabled when not in use. ■ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ■ Enabled only during the time period needed and disabled when not in use. ■ Use is monitored for unexpected activity.	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.4.3	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ■ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ■ All remote access by third parties and vendors.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.4.3	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ■ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ■ All remote access by third parties and vendors.	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	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.4.3	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ■ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ■ All remote access by third parties and vendors.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 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 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 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: ■ 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.
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 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 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 up 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.
9.2.2	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.2.2	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.2.2	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	Media are classified and protected appropriately.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	Media are classified and protected appropriately.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ■ Media sent outside the facility is logged. ■ Media is sent by secured courier or other delivery method that can be accurately tracked. ■ Offsite tracking logs include details about media location.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	Media is secured and tracked when transported outside the facility.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ■ Media sent outside the facility is logged. ■ Media is sent by secured courier or other delivery method that can be accurately tracked. ■ Offsite tracking logs include details about media location.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	Media is secured and tracked when transported outside the facility.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive/regulated media that is transferred outside of the organization's facilities.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ■ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ■ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ■ Maintaining a list of POI devices. ■ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ■ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where:(1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and(2) Physical assessments evaluate assets for evidence of unauthorized access and/or modifications.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The identity and location of POI devices is recorded and known at all times.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	5	The identity and location of POI devices is recorded and known at all times.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The identity and location of POI devices is recorded and known at all times.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Kiosks & Point of Interaction (POI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	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	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Network Segmentation (macrosegementation)	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	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	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	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
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.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	Personnel understand their role in protecting the entity's cardholder data.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.

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
12.6.1	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.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:(1) Contractual obligations for the External Service Provider (ESP);(2) Business practices;(3) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	Records are maintained of TPSPs and the services provided.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.3	N/A	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.
12.8.4	N/A	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	The PCI DSS compliance status of TPSPs is verified periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
A2.1.1	N/A	Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	This requirement is not eligible for the customized approach.
A2.1.1	N/A	Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	Functional	Intersects With	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5	This requirement is not eligible for the customized approach.