

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 - SAO C
Focal Document URL: https://west.pocisecuritystandards.org/document_library/category/pocisss/document-pci-dss-4-0-1-sao-c.pdf
Published STRM URL: <https://content.securecontrolsframework.com/strm-general/pci-dss-4-0-1-sao-c.pdf>

PCI DSS v4.0.1 - SAO C
https://west.pocisecuritystandards.org/document_library/category/pocisss/document-pci-dss-4-0-1-sao-c.pdf
<https://content.securecontrolsframework.com/strm-general/pci-dss-4-0-1-sao-c.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.3.1	NA	Inbound traffic to the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Inbound traffic to the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Inbound traffic to the CDE is restricted as follows: <ul style="list-style-type: none"> To only traffic that is necessary. All other traffic is specifically denied. 	Functional	Intersects With	Network Segmentation (microsegmentation)	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	NA	Inbound traffic to the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> To only traffic that is necessary. All other traffic is specifically denied. 	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	Unauthorized traffic cannot leave the CDE.
1.3.2	NA	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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 (microsegmentation)	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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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	NA	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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.
2.1.1	NA	All security policies and operational procedures that are identified in Requirement 2 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	NA	All security policies and operational procedures that are identified in Requirement 2 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	NA	All security policies and operational procedures that are identified in Requirement 2 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	NA	All security policies and operational procedures that are identified in Requirement 2 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.2.1	NA	Configuration standards are developed, implemented, and maintained to: <ul style="list-style-type: none"> Cover all system components. Address all known security vulnerabilities. Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. Be updated as new vulnerability issues are identified, as defined in Requirement 6.1. Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. 	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	All system components are configured secure and consistently and in accordance with industry-accepted hardening standards or vendor recommendations.
2.2.2	NA	Vendor default accounts are managed as follows: <ul style="list-style-type: none"> If the vendor default account(s) will be used, the default password is changed per Requirement 8.3. 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	NA	Vendor default accounts are managed as follows: <ul style="list-style-type: none"> If the vendor default account(s) will be used, the default password is changed per Requirement 8.3. 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.
2.2.3	NA	Primary functions requiring different security levels are managed as follows: <ul style="list-style-type: none"> Only one primary function exists on a system component, OR Primary functions with differing security levels that exist on the same system component are isolated from each other, OR Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. 	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	Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.
2.2.3	NA	Primary functions requiring different security levels are managed as follows: <ul style="list-style-type: none"> Only one primary function exists on a system component, OR Primary functions with differing security levels that exist on the same system component are isolated from each other, OR Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. 	Functional	Intersects With	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.	5	Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.
2.2.3	NA	Primary functions requiring different security levels are managed as follows: <ul style="list-style-type: none"> Only one primary function exists on a system component, OR Primary functions with differing security levels that exist on the same system component are isolated from each other, OR Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. 	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.
2.2.4	NA	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.4	NA	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.4	NA	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.5	NA	If any insecure services, protocols, or daemons are present: <ul style="list-style-type: none"> Business justification is documented. Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. 	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	System components cannot be compromised by exploiting insecure services, protocols, or daemons.
2.2.5	NA	If any insecure services, protocols, or daemons are present: <ul style="list-style-type: none"> Business justification is documented. Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. 	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols, and services necessary to operate technology solutions.	5	System components cannot be compromised by exploiting insecure services, protocols, or daemons.
2.2.6	NA	System security parameters are configured to prevent misuse.	Functional	Intersects With	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.	5	System components cannot be compromised because of incorrect security parameter configuration.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Content Description	Strength of Relationship	Notes
2.2.7	NA	All non-console administrative access is encrypted using strong cryptography.	Functional	Subset Of	Use of Cryptographic Controls Through Cryptographic Modules	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered uncollectible 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	NA	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	NA	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	NA	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/regulating 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	NA	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	NA	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Data Masking	PR-05.3	Mechanisms exist to mask sensitive/regulating data through data anonymization, pseudonymization, redaction or de-identification.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
4.2.1	NA	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: ■ Only trusted keys and certificates are accepted. ■ Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. ■ The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. ■ The encryption strength is appropriate for the encryption methodology in use.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.
4.2.1	NA	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: ■ Only trusted keys and certificates are accepted. ■ Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. ■ The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. ■ The encryption strength is appropriate for the encryption methodology in use.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulating data during transmission over open, public networks.	5	Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.
4.2.1	NA	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: ■ Only trusted keys and certificates are accepted. ■ Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. ■ The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. ■ The encryption strength is appropriate for the encryption methodology in use.	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	Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.
4.2.1.2	NA	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.1.2	NA	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.1.2	NA	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.2	NA	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	Functional	Intersects With	End-User Messaging Technologies	NET-12.2	Mechanisms exist to prohibit the transmission of unprotected sensitive/regulating data by end-user messaging technologies.	5	Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.
5.1.1	NA	All security policies and operational procedures that are identified in Requirement 5 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 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
5.1.1	NA	All security policies and operational procedures that are identified in Requirement 5 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 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
5.1.1	NA	All security policies and operational procedures that are identified in Requirement 5 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 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.1.1	NA	All security policies and operational procedures that are identified in Requirement 5 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
5.2.1	NA	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.2 that concludes the system components are not at risk from malware.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.
5.2.2	NA	The deployed anti-malware solution(s): <ul style="list-style-type: none"> Detects all known types of malware. Removes, blocks, or contains all known types of malware. 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Malware cannot execute or infect other system components.
5.2.3	NA	Any system components that are not at risk for malware are evaluated periodically to include the following: <ul style="list-style-type: none"> A documented list of all system components not at risk for malware. Identification and evaluation of evolving malware threats for those system components. Confirmation whether such system components continue to not require anti-malware protection. 	Functional	Intersects With	Evolving Malware Threats	END-04.6	Mechanisms exist to perform periodic evaluations evolving malware threats to assess systems that are generally not considered to be commonly affected by malicious software.	5	The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.
5.2.3.1	NA	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	Functional	Intersects With	Evolving Malware Threats	END-04.6	Mechanisms exist to perform periodic evaluations evolving malware threats to assess systems that are generally not considered to be commonly affected by malicious software.	5	Systems not known to be at risk from malware are re-evaluated at a frequency that addresses the entity's risk.
5.3.1	NA	The anti-malware solution(s) is kept current via automatic updates.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Anti-malware mechanisms can detect and address the latest malware threats.
5.3.1	NA	The anti-malware solution(s) is kept current via automatic updates.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update anti-malware technologies, including signature definitions.	5	Anti-malware mechanisms can detect and address the latest malware threats.
5.3.2	NA	The anti-malware solution(s): <ul style="list-style-type: none"> Performs periodic scans and active or real-time scans. OR Performs continuous behavioral analysis of systems or processes. 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Malware cannot complete execution.
5.3.2	NA	The anti-malware solution(s): <ul style="list-style-type: none"> Performs periodic scans and active or real-time scans. OR Performs continuous behavioral analysis of systems or processes. 	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Malware cannot complete execution.
5.3.2.1	NA	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Scans by the malware solution are performed at a frequency that addresses the entity's risk.
5.3.2.1	NA	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Scans by the malware solution are performed at a frequency that addresses the entity's risk.
5.3.3	NA	For removable electronic media, the anti-malware solution(s): <ul style="list-style-type: none"> Performs automatic scans of when the media is inserted, connected, or logically mounted. OR Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Malware cannot be introduced to system components via external removable media.
5.3.3	NA	For removable electronic media, the anti-malware solution(s): <ul style="list-style-type: none"> Performs automatic scans of when the media is inserted, connected, or logically mounted. OR Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. 	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Malware cannot be introduced to system components via external removable media.
5.3.4	NA	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Historical records of anti-malware actions are immediately available and retained for at least 12 months.
5.3.4	NA	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage anti-malware technologies.	5	Historical records of anti-malware actions are immediately available and retained for at least 12 months.
5.3.5	NA	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	Anti-malware mechanisms cannot be modified by unauthorized personnel.
5.3.5	NA	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Anti-malware mechanisms cannot be modified by unauthorized personnel.
5.4.1	NA	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	Functional	Intersects With	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Intersects With	Threat Analysis & Flow 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	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that(1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;(2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and(3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	NA	Bespoke and custom software are developed securely, as follows: <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. In accordance with PCI DSS (for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle. 	Functional	Intersects With	Developer Threat Analysis & Flow Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Threat Analysis & Flow 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	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	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; and(3) Annually thereafter.	5	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Continuing Professional Education (CPE) DevOps Personnel	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	5	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel 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
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	5	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.2	NA	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	Functional	Intersects With	Developer Threat Analysis & 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	Software development personnel remain knowledgeable about secure development practices, software security, and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.
6.2.3.1	NA	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: <ul style="list-style-type: none"> Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. Reviewed and approved by management prior to release. 	Functional	Intersects With	Threat Analysis & 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	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.3.1	NA	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: <ul style="list-style-type: none"> Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. Reviewed and approved by management prior to release. 	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flow remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.3.1	NA	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: <ul style="list-style-type: none"> Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. Reviewed and approved by management prior to release. 	Functional	Intersects With	Developer Threat Analysis & 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	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flow remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Threat Analysis & 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	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.

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
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attempts on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attempts on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attempts on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attempts on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attempts via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attempts on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attempts on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attempts on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attempts on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attempts via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	NA	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: <ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. Attempts on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. Attempts on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. Attempts on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). Attempts on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. Attempts via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	Functional	Intersects With	Developer Threat Analysis & 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	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Threat Analysis & Flow Remediation During Development	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	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to (1) facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Developer Threat Analysis & Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

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	NA	Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> New security vulnerabilities are identified using industry recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.3	NA	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: <ul style="list-style-type: none"> Critical or high-security patches/updates identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). 	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	NA	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: <ul style="list-style-type: none"> Critical or high-security patches/updates identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). 	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	NA	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: <ul style="list-style-type: none"> Critical or high-security patches/updates identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). 	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	NA	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: <ul style="list-style-type: none"> Critical or high-security patches/updates identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). 	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.5.1	NA	Changes to all system components in the production environment are made according to established procedures that include: <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.1	NA	Changes to all system components in the production environment are made according to established procedures that include: <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.1	NA	Changes to all system components in the production environment are made according to established procedures that include: <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.1	NA	Changes to all system components in the production environment are made according to established procedures that include: <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.1	NA	Changes to all system components in the production environment are made according to established procedures that include: <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	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	All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	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	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a production environment.	5	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Functional	Intersects With	Report Verification Results	CHG-06.1	Mechanisms exist to report the results of security, compliance and resilience capability verification to appropriate organizational management.	5	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	NA	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	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	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
7.2.2	NA	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> job classification and function. Least privileges necessary to perform job responsibilities. 	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	NA	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> job classification and function. Least privileges necessary to perform job responsibilities. 	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	NA	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> job classification and function. Least privileges necessary to perform job responsibilities. 	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	NA	Access is assigned to users, including privileged users, based on: <ul style="list-style-type: none"> job classification and function. Least privileges necessary to perform job responsibilities. 	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.3	NA	Required privileges are approved by authorized personnel.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	Access privileges cannot be granted to users without appropriate, documented authorization.
7.2.3	NA	Required privileges are approved by authorized personnel.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	Access privileges cannot be granted to users without appropriate, documented authorization.
7.2.3	NA	Required privileges are approved by authorized personnel.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Access privileges cannot be granted to users without appropriate, documented authorization.
7.2.3	NA	Required privileges are approved by authorized personnel.	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	Access privileges cannot be granted to users without appropriate, documented authorization.
7.2.4	NA	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: <ul style="list-style-type: none"> At least once every six months. To ensure user accounts and access remain appropriate based on job function. Any inappropriate access is addressed. Management acknowledges that access remains appropriate. 	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.
7.2.4	NA	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: <ul style="list-style-type: none"> At least once every six months. To ensure user accounts and access remain appropriate based on job function. Any inappropriate access is addressed. Management acknowledges that access remains appropriate. 	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.
7.2.5	NA	All application and system accounts and related access privileges are assigned and managed as follows: <ul style="list-style-type: none"> Based on the least privileges necessary for the operability of the system or application. Access is limited to the systems, applications, or processes that specifically require their use. 	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 rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.

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
7.2.5	NA	All application and system accounts and related access privileges are assigned and managed as follows: ■ Based on the least privileges necessary for the operability of the system or application. ■ Access is limited to the systems, applications, or processes that specifically require their use.	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 rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.
7.2.5	NA	All application and system accounts and related access privileges are assigned and managed as follows: ■ Based on the least privileges necessary for the operability of the system or application. ■ Access is limited to the systems, applications, or processes that specifically require their use.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.
7.2.5	NA	All application and system accounts and related access privileges are assigned and managed as follows: ■ Based on the least privileges necessary for the operability of the system or application. ■ Access is limited to the systems, applications, or processes that specifically require their use.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.
7.2.5	NA	All application and system accounts and related access privileges are assigned and managed as follows: ■ Based on the least privileges necessary for the operability of the system or application. ■ Access is limited to the systems, applications, or processes that specifically require their use.	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 rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.
8.1.1	NA	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	NA	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 (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 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	NA	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	NA	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.
8.2.1	NA	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	All actions by all users are attributable to an individual.
8.2.1	NA	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	All actions by all users are attributable to an individual.
8.2.2	NA	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	NA	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	NA	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.
8.2.4	NA	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ■ Authorized with the appropriate approval. ■ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.4	NA	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ■ Authorized with the appropriate approval. ■ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.4	NA	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ■ Authorized with the appropriate approval. ■ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.4	NA	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ■ Authorized with the appropriate approval. ■ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.4	NA	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ■ Authorized with the appropriate approval. ■ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.5	NA	Access for terminated users is immediately revoked.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	The accounts of terminated users cannot be used.
8.2.5	NA	Access for terminated users is immediately revoked.	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	The accounts of terminated users cannot be used.
8.2.5	NA	Access for terminated users is immediately revoked.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	The accounts of terminated users cannot be used.
8.2.5	NA	Access for terminated users is immediately revoked.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	The accounts of terminated users cannot be used.
8.2.5	NA	Access for terminated users is immediately revoked.	Functional	Intersects With	Revocation of Access Authorizations	IAC-06	Mechanisms exist to revoke logical and physical access authorizations.	5	The accounts of terminated users cannot be used.
8.2.6	NA	Inactive user accounts are removed or disabled within 90 days of inactivity.	Functional	Intersects With	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	Inactive user accounts cannot be used.
8.2.7	NA	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	NA	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	NA	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.
8.2.7	NA	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	NA	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.
8.2.8	NA	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	Functional	Intersects With	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	5	A user session cannot be used except by the authorized user.
8.2.8	NA	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	A user session cannot be used except by the authorized user.
8.2.8	NA	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	Functional	Intersects With	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	A user session cannot be used except by the authorized user.
8.2.8	NA	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	Functional	Intersects With	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5	A user session cannot be used except by the authorized user.
8.3.1	NA	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.3.1	NA	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.1	NA	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ■ Something you know, such as a password or passphrase. ■ Something you have, such as a token device or smart card. ■ Something you are, such as a biometric element.	Functional	Intersects With	PKI-Based Authentication	IAC.10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.2	NA	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	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 authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.
8.3.2	NA	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	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	Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.
8.3.2	NA	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.
8.3.2	NA	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.
8.3.3	NA	User identity is verified before modifying any authentication factor.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
8.3.3	NA	User identity is verified before modifying any authentication factor.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
8.3.3	NA	User identity is verified before modifying any authentication factor.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
8.3.3	NA	User identity is verified before modifying any authentication factor.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
8.3.3	NA	User identity is verified before modifying any authentication factor.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC.28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5	
8.3.4	NA	Invalid authentication attempts are limited by: ■ Locking out the user ID after not more than 10 attempts. ■ Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	An authentication factor cannot be guessed in a brute force, online attack.
8.3.5	NA	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	NA	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	NA	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ■ Set to a unique value for first-time use and upon reset. ■ Forced to be changed immediately after the first use.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.6	NA	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: ■ A minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters). ■ Contain both numeric and alphabetic characters.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A guessed password/passphrase cannot be verified by either an online or offline brute force attack.
8.3.7	NA	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.7	NA	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	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	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	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	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	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	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	NA	Authentication policies and procedures are documented and communicated to all users including: ■ Guidance on selecting strong authentication factors. ■ Guidance for how users should protect their authentication factors. ■ Instructions not to reuse previously used password/passphrases. ■ Instructions to change password/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	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 performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.9	NA	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.3.9	NA	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.3.9	NA	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ■ Passwords/passphrases are changed at least once every 90 days, OR ■ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Password-Based Authentication	IAC.10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.4.1	NA	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	Administrative access to the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	NA	MFA is implemented for all access into the CDE.	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 (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data.	5	Access into the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	NA	MFA is implemented for all access into the CDE.	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	Access into the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	NA	MFA is implemented for all access into the CDE.	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	Access into the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	NA	MFA is implemented for all access into the CDE.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	Access into the CDE cannot be obtained by the use of a single authentication factor.

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
8.4.2	NA	MFA is implemented for all access into the CDE.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	Access into the CDE cannot be obtained by the use of a single authentication factor.
8.4.3	NA	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: <ul style="list-style-type: none"> 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/regulatory data.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.4.3	NA	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: <ul style="list-style-type: none"> 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	NA	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: <ul style="list-style-type: none"> 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.
8.5.1	NA	MFA systems are implemented as follows: <ul style="list-style-type: none"> The MFA system is not susceptible to replay attacks. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. At least two different types of authentication factors are used. Success of all authentication factors is required before access is granted. 	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	MFA systems are resistant to attack and strictly control any administrative overrides.
8.5.1	NA	MFA systems are implemented as follows: <ul style="list-style-type: none"> The MFA system is not susceptible to replay attacks. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. At least two different types of authentication factors are used. Success of all authentication factors is required before access is granted. 	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	MFA systems are resistant to attack and strictly control any administrative overrides.
8.5.1	NA	MFA systems are implemented as follows: <ul style="list-style-type: none"> The MFA system is not susceptible to replay attacks. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. At least two different types of authentication factors are used. Success of all authentication factors is required before access is granted. 	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/regulatory data.	5	MFA systems are resistant to attack and strictly control any administrative overrides.
8.5.1	NA	MFA systems are implemented as follows: <ul style="list-style-type: none"> The MFA system is not susceptible to replay attacks. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. At least two different types of authentication factors are used. Success of all authentication factors is required before access is granted. 	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	MFA systems are resistant to attack and strictly control any administrative overrides.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	Functional	Intersects With	Sharing Identification & Authentication Information	IAC-05.1	Mechanisms exist to ensure external service providers provide current and accurate information for any third-party user system or application accounts that are authorized and attributable to an individual person.	5	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	Functional	Intersects With	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any accounts that cannot be associated with a business process and owner.	5	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to 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	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	Functional	Intersects With	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	5	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.1	NA	If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for the exceptional circumstance. Business justification for interactive use is documented. Interactive use is explicitly approved by management. Individual user identity is confirmed before access to account is granted. Every action taken is attributable to an individual user. 	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	When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.
8.6.2	NA	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	5	Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.
8.6.3	NA	Passwords/passphrases for any application and system accounts are protected against misuse as follows: <ul style="list-style-type: none"> Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the password/passphrases. 	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.
8.6.3	NA	Passwords/passphrases for any application and system accounts are protected against misuse as follows: <ul style="list-style-type: none"> Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the password/passphrases. 	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.
9.1.1	NA	All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.1	NA	All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.1	NA	All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9.1.1	NA	All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> Documented Kept up to date. In use Known to all affected parties. 	Functional	Intersects With	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	NA	All security policies and operational procedures that are identified in Requirement 9 are: <ul style="list-style-type: none"> Documented Kept up to date. In use Known to all affected parties. 	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.2.1	NA	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1	NA	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1	NA	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) at facilities (excluding those areas within the facility officially designated as publicly accessible).	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1	NA	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1	NA	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1.1	NA	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: <ul style="list-style-type: none"> Entry and exit points to/from sensitive areas within the CDE are monitored. Monitoring devices or mechanisms are protected from tampering or disabling. Collected data is reviewed and correlated with other entries. Collected data is stored for at least three months, unless otherwise restricted by law. 	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.
9.2.1.1	NA	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: <ul style="list-style-type: none"> Entry and exit points to/from sensitive areas within the CDE are monitored. Monitoring devices or mechanisms are protected from tampering or disabling. Collected data is reviewed and correlated with other entries. Collected data is stored for at least three months, unless otherwise restricted by law. 	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.
9.2.1.1	NA	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: <ul style="list-style-type: none"> Entry and exit points to/from sensitive areas within the CDE are monitored. Monitoring devices or mechanisms are protected from tampering or disabling. Collected data is reviewed and correlated with other entries. Collected data is stored for at least three months, unless otherwise restricted by law. 	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.
9.2.1.1	NA	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: <ul style="list-style-type: none"> Entry and exit points to/from sensitive areas within the CDE are monitored. Monitoring devices or mechanisms are protected from tampering or disabling. Collected data is reviewed and correlated with other entries. Collected data is stored for at least three months, unless otherwise restricted by law. 	Functional	Intersects With	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	5	Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.
9.2.2	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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	NA	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 sensitive 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	NA	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	NA	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	NA	Media with cardholder data sent outside the facility is secured as follows: <ul style="list-style-type: none"> Media sent outside the facility is logged. Media is sent by secured courier or other delivery method that can be accurately tracked. Offline 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	NA	Media with cardholder data sent outside the facility is secured as follows: <ul style="list-style-type: none"> Media sent outside the facility is logged. Media is sent by secured courier or other delivery method that can be accurately tracked. Offline 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	NA	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	NA	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 security-related information that is transferred outside of the organization's facilities.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.6	NA	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: <ul style="list-style-type: none"> 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 fulfil the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroy, erase, and/or anonymize the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	NA	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: <ul style="list-style-type: none"> 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	NA	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: <ul style="list-style-type: none"> 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> 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.

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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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/regulatory 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.
9.5.1	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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/regulatory 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	NA	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: <ul style="list-style-type: none"> ● 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	NA	An up-to-date list of POI devices is maintained, including: <ul style="list-style-type: none"> ● 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	NA	An up-to-date list of POI devices is maintained, including: <ul style="list-style-type: none"> ● 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 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	NA	An up-to-date list of POI devices is maintained, including: <ul style="list-style-type: none"> ● 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/regulatory 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	NA	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/regulatory 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	NA	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	NA	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	NA	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> ● 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	NA	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> ● 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	NA	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> ● 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	NA	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> ● 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/regulatory 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	NA	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> ● 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.
10.1.1	NA	All security policies and operational procedures that are identified in Requirement 10 are: <ul style="list-style-type: none"> ● Documented. ● Kept up to date. ● In use. ● Known to all affected parties. 	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
10.1.1	NA	All security policies and operational procedures that are identified in Requirement 10 are: <ul style="list-style-type: none"> ● Documented. ● Kept up to date. ● In use. ● Known to all affected parties. 	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
10.1.1	NA	All security policies and operational procedures that are identified in Requirement 10 are: <ul style="list-style-type: none"> ● Documented. ● Kept up to date. ● In use. ● Known to all affected parties. 	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
10.1.1	NA	All security policies and operational procedures that are identified in Requirement 10 are: <ul style="list-style-type: none"> Documented. Kept up to date. In use. Known to all affected parties. 	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	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	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	Auditing Use of Privileged Functions	IAC-2.4	Mechanisms exist to audit the execution of privileged functions.	5	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	5	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.2	NA	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	Records of all actions performed by individuals with elevated privileges are captured.
10.2.1.4	NA	Audit logs capture all invalid logical access attempts.	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	Records of all invalid access attempts are captured.
10.2.1.4	NA	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all invalid access attempts are captured.
10.2.1.4	NA	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	5	Records of all invalid access attempts are captured.
10.2.1.4	NA	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all invalid access attempts are captured.
10.2.1.4	NA	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	Records of all invalid access attempts are captured.
10.2.1.5	NA	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> Creation of new accounts. Elevation of privileges. All changes, additions, or deletions to accounts with administrative access. 	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	5	Records of all changes to identification and authentication credentials are captured.
10.2.1.5	NA	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> Creation of new accounts. Elevation of privileges. All changes, additions, or deletions to accounts with administrative access. 	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all changes to identification and authentication credentials are captured.
10.2.1.5	NA	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> Creation of new accounts. Elevation of privileges. All changes, additions, or deletions to accounts with administrative access. 	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	Records of all changes to identification and authentication credentials are captured.
10.2.1.5	NA	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> Creation of new accounts. Elevation of privileges. All changes, additions, or deletions to accounts with administrative access. 	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	Records of all changes to identification and authentication credentials are captured.
10.2.1.5	NA	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> Creation of new accounts. Elevation of privileges. All changes, additions, or deletions to accounts with administrative access. 	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all changes to identification and authentication credentials are captured.
10.2.2	NA	Audit logs record the following details for each auditable event: <ul style="list-style-type: none"> User identification. Type of event. Date and time. Success and failure indication. Origin of event. Identity or name of affected data, system component, resource, or service (for example, name and protocol). 	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	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.2.1 are captured.
10.2.2	NA	Audit logs record the following details for each auditable event: <ul style="list-style-type: none"> User identification. Type of event. Date and time. Success and failure indication. Origin of event. Identity or name of affected data, system component, resource, or service (for example, name and protocol). 	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.2.1 are captured.
10.2.2	NA	Audit logs record the following details for each auditable event: <ul style="list-style-type: none"> User identification. Type of event. Date and time. Success and failure indication. Origin of event. Identity or name of affected data, system component, resource, or service (for example, name and protocol). 	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	5	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.2.1 are captured.
10.2.2	NA	Audit logs record the following details for each auditable event: <ul style="list-style-type: none"> User identification. Type of event. Date and time. Success and failure indication. Origin of event. Identity or name of affected data, system component, resource, or service (for example, name and protocol). 	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.2.1 are captured.
10.3.1	NA	Read access to audit logs files is limited to those with a job-related need.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	Stored activity records cannot be accessed by unauthorized personnel.
10.3.1	NA	Read access to audit logs files is limited to those with a job-related need.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	5	Stored activity records cannot be accessed by unauthorized personnel.
10.3.1	NA	Audit logs files are protected to prevent modifications by individuals.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	Stored activity records cannot be modified by personnel.
10.3.2	NA	Audit logs files are protected to prevent modifications by individuals.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	5	Stored activity records cannot be modified by personnel.
10.3.3	NA	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Stored activity records are secured and preserved in a central location to prevent unauthorized modification.
10.3.3	NA	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	Stored activity records are secured and preserved in a central location to prevent unauthorized modification.
10.3.3	NA	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	Stored activity records are secured and preserved in a central location to prevent unauthorized modification.
10.3.4	NA	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to protected files and configuration settings.	5	Stored activity records cannot be modified without an alert being generated.
10.3.4	NA	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	Stored activity records cannot be modified without an alert being generated.
10.4.1	NA	The following audit logs are reviewed at least once daily: <ul style="list-style-type: none"> All security events. Logs of all system components that store, process, or transmit CHD and/or S&D. Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). 	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.
10.4.1	NA	The following audit logs are reviewed at least once daily: <ul style="list-style-type: none"> All security events. Logs of all system components that store, process, or transmit CHD and/or S&D. Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). 	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.
10.4.1	NA	The following audit logs are reviewed at least once daily: <ul style="list-style-type: none"> All security events. Logs of all system components that store, process, or transmit CHD and/or S&D. Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). 	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.
10.4.1	NA	The following audit logs are reviewed at least once daily: <ul style="list-style-type: none"> All security events. Logs of all system components that store, process, or transmit CHD and/or S&D. Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). 	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.

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
10.4.1	NA	The following audit logs are reviewed at least once daily: ■ All security events. ■ Logs of all system components that store, process, or transmit CHD and/or S&D. ■ Logs of all critical system components. ■ Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection system/intrusion-prevention systems (IDS/IPS), authentication servers).	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.1.1	NA	Automated mechanisms are used to perform audit log reviews.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.
10.4.2	NA	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.
10.4.2.1	NA	The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Log reviews for lower-risk system components are performed at a frequency that addresses the entity's risk.
10.4.3	NA	Exceptions and anomalies identified during the review process are addressed.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Suspicious or anomalous activities are addressed.
10.4.3	NA	Exceptions and anomalies identified during the review process are addressed.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	Suspicious or anomalous activities are addressed.
10.4.3	NA	Exceptions and anomalies identified during the review process are addressed.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Suspicious or anomalous activities are addressed.
10.5.1	NA	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	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	Historical records of activity are available immediately to support incident response and are retained for at least 12 months.
10.5.1	NA	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	Historical records of activity are available immediately to support incident response and are retained for at least 12 months.
10.5.1	NA	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PR-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, destroy, erase, and/or anonymize the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Historical records of activity are available immediately to support incident response and are retained for at least 12 months.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	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	Common time is established across all systems.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas with more restrictive baseline configurations.	5	Common time is established across all systems.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	Common time is established across all systems.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	Common time is established across all systems.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	Common time is established across all systems.
10.6.1	NA	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	Common time is established across all systems.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	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 time on all systems is accurate and consistent.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	The time on all systems is accurate and consistent.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	The time on all systems is accurate and consistent.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	The time on all systems is accurate and consistent.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	The time on all systems is accurate and consistent.
10.6.2	NA	Systems are configured to the correct and consistent time as follows: ■ One or more designated time servers are in use. ■ Only the designated central time server(s) receives time from external sources. ■ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). ■ The designated time server(s) accept time updates only from specific industry-accepted external sources. ■ Where there is more than one designated time server, the time servers peer with one another to keep accurate time. ■ Internal systems receive time information only from designated central time server(s).	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	The time on all systems is accurate and consistent.
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	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	System time settings cannot be modified by unauthorized personnel.
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas with more restrictive baseline configurations.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	System time settings cannot be modified by unauthorized 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
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	NA	Time synchronization settings and data are protected as follows: ■ Access to time data is restricted to only personnel with a business need. ■ Any changes to time settings on critical systems are logged, monitored, and reviewed.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	System time settings cannot be modified by unauthorized personnel.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	Unauthorized wireless access points are identified and addressed periodically.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	Unauthorized wireless access points are identified and addressed periodically.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	5	Unauthorized wireless access points are identified and addressed periodically.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	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 wireless access points are identified and addressed periodically.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	Unauthorized wireless access points are identified and addressed periodically.
11.2.1	NA	Authorized and unauthorized wireless access points are managed as follows: ■ The presence of wireless (Wi-Fi) access points is tested for. ■ All authorized and unauthorized wireless access points are detected and identified. ■ Testing, detection, and identification occurs at least once every three months. ■ If automated monitoring is used, personnel are notified via generated alerts.	Functional	Intersects With	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	5	Unauthorized wireless access points are identified and addressed periodically.
11.2.2	NA	An inventory of authorized wireless access points is maintained, including a documented business justification.	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	Unauthorized wireless access points are not mistaken for authorized wireless access points.
11.2.2	NA	An inventory of authorized wireless access points is maintained, including a documented business justification.	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	Unauthorized wireless access points are not mistaken for authorized wireless access points.
11.2.2	NA	An inventory of authorized wireless access points is maintained, including a documented business justification.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	Unauthorized wireless access points are not mistaken for authorized wireless access points.
11.2.2	NA	An inventory of authorized wireless access points is maintained, including a documented business justification.	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 wireless access points are not mistaken for authorized wireless access points.
11.2.2	NA	An inventory of authorized wireless access points is maintained, including a documented business justification.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	Unauthorized wireless access points are not mistaken for authorized wireless access points.
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Attack Surface Scope	VPM-01	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1	NA	Internal vulnerability scans are performed as follows: ■ At least once every three months. ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. ■ Scan tool is kept up to date with latest vulnerability information. ■ Scans are performed by qualified personnel and organizational independence of the tester exists.	Functional	Intersects With	Internal Vulnerability Assessment Scans	VPM-06.7	Mechanisms exist to perform quarterly internal vulnerability scans, which includes all segments of the organization's internal network, as well as rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.(continued on next page)
11.3.1.3	NA	Internal vulnerability scans are performed after any significant change as follows: ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.1.3	NA	Internal vulnerability scans are performed after any significant change as follows: ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.1.3	NA	Internal vulnerability scans are performed after any significant change as follows: ■ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. ■ Rescans are performed as needed. ■ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.

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
11.3.1.3	NA	Internal vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	Internal Vulnerability Assessment Scans	VPM-06.7	Mechanisms exist to perform quarterly internal vulnerability scans, which includes all segments of the organization's internal network, as well as rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2	NA	External vulnerability scans are performed as follows: <ul style="list-style-type: none"> 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	NA	External vulnerability scans are performed as follows: <ul style="list-style-type: none"> 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	NA	External vulnerability scans are performed as follows: <ul style="list-style-type: none"> 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	NA	External vulnerability scans are performed as follows: <ul style="list-style-type: none"> At least once every three months. By a PCI SSC Approved Scanning Vendor (ASV). Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan. 	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	This requirement is not eligible for the customized approach.
11.3.2.1	NA	External vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	NA	External vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	NA	External vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that defines the system components scanned and types of vulnerabilities that are checked for.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	NA	External vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	NA	External vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. Rescans are conducted as needed. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.4.5	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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 (microsegmentation)	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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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 Demilitarized 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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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	

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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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	NA	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> 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.
11.5.2	NA	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: <ul style="list-style-type: none"> To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. To perform critical file comparisons at least once weekly. 	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected file and configuration settings.	5	Critical files cannot be modified by unauthorized personnel without an alert being generated.
11.5.2	NA	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: <ul style="list-style-type: none"> To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. To perform critical file comparisons at least once weekly. 	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-07.1	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	Critical files cannot be modified by unauthorized personnel without an alert being generated.
12.1.1	NA	An overall information security policy is: <ul style="list-style-type: none"> 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	NA	An overall information security policy is: <ul style="list-style-type: none"> 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 (SCR), 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	NA	The information security policy is: <ul style="list-style-type: none"> 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	NA	The information security policy is: <ul style="list-style-type: none"> 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 (SCR), 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	NA	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	NA	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 (SCR).	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	NA	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	NA	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	NA	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	NA	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.
12.2.1	NA	Acceptable use policies for end-user technologies are documented and implemented, including: <ul style="list-style-type: none"> Explicit approval by authorized parties. Acceptable uses of the technology. List of products approved by the company for employee use, including hardware and software. 	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	The use of end-user technologies is defined and managed to ensure authorized usage.
12.2.1	NA	Acceptable use policies for end-user technologies are documented and implemented, including: <ul style="list-style-type: none"> Explicit approval by authorized parties. Acceptable uses of the technology. List of products approved by the company for employee use, including hardware and software. 	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	The use of end-user technologies is defined and managed to ensure authorized usage.
12.2.1	NA	Acceptable use policies for end-user technologies are documented and implemented, including: <ul style="list-style-type: none"> Explicit approval by authorized parties. Acceptable uses of the technology. List of products approved by the company for employee use, including hardware and software. 	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	The use of end-user technologies is defined and managed to ensure authorized usage.
12.2.1	NA	Acceptable use policies for end-user technologies are documented and implemented, including: <ul style="list-style-type: none"> Explicit approval by authorized parties. Acceptable uses of the technology. List of products approved by the company for employee use, including hardware and software. 	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	The use of end-user technologies is defined and managed to ensure authorized usage.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threats that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threats that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threats that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threats that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Up to date knowledge and assessment of risks to the CDE are maintained.

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
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threat(s) that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threat(s) that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threat(s) that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threat(s) that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	NA	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: <ul style="list-style-type: none"> Identification of the assets being protected. Identification of the threat(s) that the requirement is protecting against. Identification of factors that contribute to the likelihood and/or impact of a threat being realized. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. Performance of updated risk analyses when needed, as determined by the annual review. 	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.6.1	NA	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	NA	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	NA	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	NA	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including (1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.3.1	NA	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	NA	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	NA	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	NA	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	NA	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.8.1	NA	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	NA	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	NA	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	NA	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	NA	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:(1) Contractual obligations for the External Service Provider (ESP);(2) Business practices;(3) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	Records are maintained of TPSPs and the services provided.
12.8.2	NA	Written agreements with TPSPs are maintained as follows: <ul style="list-style-type: none"> Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. 	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	NA	Written agreements with TPSPs are maintained as follows: <ul style="list-style-type: none"> 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	NA	Written agreements with TPSPs are maintained as follows: <ul style="list-style-type: none"> 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	NA	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.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
12.8.4	NA	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	NA	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	NA	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.10.1	NA	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: <ul style="list-style-type: none"> 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	NA	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: <ul style="list-style-type: none"> 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	IRS-03	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	NA	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: <ul style="list-style-type: none"> 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	NA	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: <ul style="list-style-type: none"> 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	NA	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: <ul style="list-style-type: none"> 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.
12.10.3	NA	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	Incidents are responded to immediately where appropriate.
A2.1.1	NA	Where POS PDI 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	NA	Where POS PDI 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.