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

Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

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

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	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	
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	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	
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
1.1	N/A	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
1.1.1	N/A	All security policies and operational procedures that are identified in Requirement 1 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
1.1.1	N/A	All security policies and operational procedures that are identified in Requirement 1 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
1.1.1	N/A	All security policies and operational procedures that are identified in Requirement 1 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 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
1.1.1	N/A	All security policies and operational procedures that are identified in Requirement 1 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 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
1.1.2	N/A	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
1.1.2	N/A	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
1.1.2	N/A	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
1.1.2	N/A	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1.1.2	N/A	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Functional	Intersects With	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
1.2	N/A	Network security controls (NSCs) are configured and maintained.	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	
1.2	N/A	Network security controls (NSCs) are configured and maintained.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
1.2	N/A	Network security controls (NSCs) are configured and maintained.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	The way that NSCs are configured and operate are defined and consistently applied.
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	The way that NSCs are configured and operate are defined and consistently applied.
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	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	The way that NSCs are configured and operate are defined and consistently applied.
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	The way that NSCs are configured and operate are defined and consistently applied.
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	The way that NSCs are configured and operate are defined and consistently applied.
1.2.1	N/A	Configuration standards for NSC rulesets are: ▪ Defined. ▪ Implemented. ▪ Maintained.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	The way that NSCs are configured and operate are defined and consistently applied.
1.2.2	N/A	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.
1.2.2	N/A	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.
1.2.2	N/A	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.2.3	N/A	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.
1.2.4	N/A	An accurate data-flow diagram(s) is maintained that meets the following: ▪ Shows all account data flows across systems and networks. ▪ Updated as needed upon changes to the environment.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	A representation of all transmissions of account data between system components and across network segments is maintained and available.
1.2.4	N/A	An accurate data-flow diagram(s) is maintained that meets the following: ▪ Shows all account data flows across systems and networks. ▪ Updated as needed upon changes to the environment.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	A representation of all transmissions of account data between system components and across network segments is maintained and available.
1.2.4	N/A	An accurate data-flow diagram(s) is maintained that meets the following: ▪ Shows all account data flows across systems and networks. ▪ Updated as needed upon changes to the environment.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	A representation of all transmissions of account data between system components and across network segments is maintained and available.
1.2.4	N/A	An accurate data-flow diagram(s) is maintained that meets the following: ▪ Shows all account data flows across systems and networks. ▪ Updated as needed upon changes to the environment.	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	A representation of all transmissions of account data between system components and across network segments is maintained and available.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	Identification & Justification of Ports, Protocols & Services	TDA-02.5	Mechanisms exist to require process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.5	N/A	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Functional	Intersects With	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its processes and technologies.	5	Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.6	N/A	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.
1.2.7	N/A	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	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	NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.
1.2.7	N/A	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.
1.2.7	N/A	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Functional	Intersects With	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.	5	NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.
1.2.7	N/A	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.
1.2.7	N/A	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	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	NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.
1.2.8	N/A	Configuration files for NSCs are: ▪ Secured from unauthorized access. ▪ Kept consistent with active network configurations.	Functional	Intersects With	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	5	NSCs cannot be defined or modified using untrusted configuration objects (including files).
1.2.8	N/A	Configuration files for NSCs are: ▪ Secured from unauthorized access. ▪ Kept consistent with active network configurations.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	NSCs cannot be defined or modified using untrusted configuration objects (including files).
1.2.8	N/A	Configuration files for NSCs are: ▪ Secured from unauthorized access. ▪ Kept consistent with active network configurations.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	NSCs cannot be defined or modified using untrusted configuration objects (including files).
1.2.8	N/A	Configuration files for NSCs are: ▪ Secured from unauthorized access. ▪ Kept consistent with active network configurations.	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	NSCs cannot be defined or modified using untrusted configuration objects (including files).
1.3	N/A	Network access to and from the cardholder data environment is restricted.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	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	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	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	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	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	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	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	
1.3	N/A	Network access to and from the cardholder data environment is restricted.	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	
1.3.1	N/A	Inbound traffic to the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	Unauthorized traffic cannot enter the CDE.
1.3.1	N/A	Inbound traffic to the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	Unauthorized traffic cannot enter the CDE.
1.3.1	N/A	Inbound traffic to the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Unauthorized traffic cannot enter the CDE.
1.3.1	N/A	Inbound traffic to the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Unauthorized traffic cannot enter the CDE.
1.3.2	N/A	Outbound traffic from the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	5	Unauthorized traffic cannot leave the CDE.
1.3.2	N/A	Outbound traffic from the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	Unauthorized traffic cannot leave the CDE.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.3.2	N/A	Outbound traffic from the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	Unauthorized traffic cannot leave the CDE.
1.3.2	N/A	Outbound traffic from the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Unauthorized traffic cannot leave the CDE.
1.3.2	N/A	Outbound traffic from the CDE is restricted as follows: ▪ To only traffic that is necessary. ▪ All other traffic is specifically denied.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Unauthorized traffic cannot leave the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Isolation of Information System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate systems, services and processes that support critical missions and/or business functions.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.3.3	N/A	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: ▪ All wireless traffic from wireless networks into the CDE is denied by default. ▪ Only wireless traffic with an authorized business purpose is allowed into the CDE.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.
1.4	N/A	Network connections between trusted and untrusted networks are controlled.	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	
1.4	N/A	Network connections between trusted and untrusted networks are controlled.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
1.4	N/A	Network connections between trusted and untrusted networks are controlled.	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	
1.4	N/A	Network connections between trusted and untrusted networks are controlled.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	
1.4	N/A	Network connections between trusted and untrusted networks are controlled.	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	
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	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 trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.1	N/A	NSCs are implemented between trusted and untrusted networks.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems.	5	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	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	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	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	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	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	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.2	N/A	Inbound traffic from untrusted networks to trusted networks is restricted to: ▪ Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. ▪ Stateful responses to communications initiated by system components in a trusted network. ▪ All other traffic is denied.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.3	N/A	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS)	NET-08.2	Mechanisms exist to monitor wireless network segments to implement Wireless Intrusion Detection / Prevention Systems (WIDS/WIPS) technologies.	5	Packets with forged IP source addresses cannot enter a trusted network.
1.4.4	N/A	System components that store cardholder data are not directly accessible from untrusted networks.	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	Stored cardholder data cannot be accessed from untrusted networks.
1.4.4	N/A	System components that store cardholder data are not directly accessible from untrusted networks.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	Stored cardholder data cannot be accessed from untrusted networks.
1.4.5	N/A	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	Functional	Intersects With	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.	5	Internal network information is protected from unauthorized disclosure.
1.4.5	N/A	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	Functional	Intersects With	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediated non-compliant systems.	5	Internal network information is protected from unauthorized disclosure.
1.5	N/A	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	Functional	Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
1.5	N/A	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
1.5	N/A	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Intersects With	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Intersects With	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external systems or service.	5	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
1.5.1	N/A	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Functional	Intersects With	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.	5	Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.
2.1	N/A	Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
2.1	N/A	Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Functional	Intersects With	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	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 (optional)	Notes (optional)
2.1.1	N/A	All security policies and operational procedures that are identified in Requirement 2 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	N/A	All security policies and operational procedures that are identified in Requirement 2 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	N/A	All security policies and operational procedures that are identified in Requirement 2 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.1	N/A	All security policies and operational procedures that are identified in Requirement 2 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
2.1.2	N/A	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
2.1.2	N/A	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
2.1.2	N/A	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
2.2	N/A	System components are configured and managed securely.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
2.2	N/A	System components are configured and managed securely.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
2.2.1	N/A	Configuration standards are developed, implemented, and maintained to: ▪ 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 6.3.1. ▪ 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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	All system components are configured securely and consistently and in accordance with industry- accepted hardening standards or vendor recommendations.
2.2.2	N/A	Vendor default accounts are managed as follows: ▪ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ▪ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	System components cannot be accessed using default passwords.
2.2.2	N/A	Vendor default accounts are managed as follows: ▪ If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. ▪ If the vendor default account(s) will not be used, the account is removed or disabled.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure vendor-supplied defaults are changed as part of the installation process. 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	N/A	Primary functions requiring different security levels are managed as follows: ▪ 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	N/A	Primary functions requiring different security levels are managed as follows: ▪ 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	N/A	Primary functions requiring different security levels are managed as follows: ▪ 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	N/A	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.4	N/A	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.4	N/A	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	System components cannot be compromised by exploiting unnecessary functionality present in the system component.
2.2.5	N/A	If any insecure services, protocols, or daemons are present: ▪ Business justification is documented. ▪ Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	System components cannot be compromised by exploiting insecure services, protocols, or daemons.
2.2.5	N/A	If any insecure services, protocols, or daemons are present: ▪ Business justification is documented. ▪ Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.	5	System components cannot be compromised by exploiting insecure services, protocols, or daemons.
2.2.6	N/A	System security parameters are configured to prevent misuse.	Functional	Intersects With	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.	5	System components cannot be compromised because of incorrect security parameter configuration.
2.2.7	N/A	All non-console administrative access is encrypted using strong cryptography.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.
2.2.7	N/A	All non-console administrative access is encrypted using strong cryptography.	Functional	Intersects With	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.
2.2.7	N/A	All non-console administrative access is encrypted using strong cryptography.	Functional	Intersects With	Non-Console Administrative Access	CRY-06	Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access.	5	Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.
2.2.7	N/A	All non-console administrative access is encrypted using strong cryptography.	Functional	Intersects With	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.	5	Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.
2.3	N/A	Wireless environments are configured and managed securely.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
2.3	N/A	Wireless environments are configured and managed securely.	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	
2.3	N/A	Wireless environments are configured and managed securely.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	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 (optional)	Notes (optional)
2.3.1	N/A	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ▪ Default wireless encryption keys. ▪ Passwords on wireless access points. ▪ SNMP defaults. ▪ Any other security-related wireless vendor defaults.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	Wireless networks cannot be accessed using vendor default passwords or default configurations.
2.3.1	N/A	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ▪ Default wireless encryption keys. ▪ Passwords on wireless access points. ▪ SNMP defaults. ▪ Any other security-related wireless vendor defaults.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure vendor-supplied defaults are changed as part of the installation process. Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	Wireless networks cannot be accessed using vendor default passwords or default configurations.
2.3.1	N/A	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ▪ Default wireless encryption keys. ▪ Passwords on wireless access points. ▪ SNMP defaults. ▪ Any other security-related wireless vendor defaults.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	Wireless networks cannot be accessed using vendor default passwords or default configurations.
2.3.1	N/A	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: ▪ Default wireless encryption keys. ▪ Passwords on wireless access points. ▪ SNMP defaults. ▪ Any other security-related wireless vendor defaults.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	Wireless networks cannot be accessed using vendor default passwords or default configurations.
2.3.2	N/A	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ▪ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ▪ Whenever a key is suspected of or known to be compromised.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.
2.3.2	N/A	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ▪ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ▪ Whenever a key is suspected of or known to be compromised.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.
2.3.2	N/A	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ▪ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ▪ Whenever a key is suspected of or known to be compromised.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.
2.3.2	N/A	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: ▪ Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. ▪ Whenever a key is suspected of or known to be compromised.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.
3.1	N/A	Processes and mechanisms for protecting stored account data are defined and understood.	Functional	Intersects With	Deactivated Account Activity	MON-01.10	Mechanisms exist to monitor deactivated accounts for attempted usage.	5	
3.1	N/A	Processes and mechanisms for protecting stored account data are defined and understood.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.1	N/A	All security policies and operational procedures that are identified in Requirement 3 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
3.1.2	N/A	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
3.1.2	N/A	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
3.1.2	N/A	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
3.2	N/A	Storage of account data is kept to a minimum.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.
3.2.1	N/A	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: ▪ Coverage for all locations of stored account data. ▪ Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. ▪ Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. ▪ Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. ▪ A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.2.1	N/A	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: ▪ Coverage for all locations of stored account data. ▪ Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. ▪ Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. ▪ Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. ▪ A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.
3.3	N/A	Sensitive authentication data (SAD) is not stored after authorization.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	
3.3.1	N/A	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.1	N/A	The full contents of any track are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.2	N/A	The card verification code is not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.1.3	N/A	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	This requirement is not eligible for the customized approach.
3.3.2	N/A	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	This requirement is not eligible for the customized approach.
3.3.2	N/A	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	This requirement is not eligible for the customized approach.
3.3.3	N/A	Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: ▪ Limited to that which is needed for a legitimate issuing business need and is secured. ▪ Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.	Functional	Intersects With	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5	Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access.
3.4	N/A	Access to displays of full PAN and ability to copy PAN is restricted.	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	
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.1	N/A	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.
3.4.2	N/A	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	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	PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.
3.4.2	N/A	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.
3.5	N/A	Primary account number (PAN) is secured wherever it is stored.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
3.5	N/A	Primary account number (PAN) is secured wherever it is stored.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
3.5.1	N/A	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: ▪ One-way hashes based on strong cryptography of the entire PAN. ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. ▪ Index tokens. ▪ Strong cryptography with associated key- management processes and procedures.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	Cleartext PAN cannot be read from storage media.
3.5.1.1	N/A	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
3.5.1.2	N/A	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: ▪ On removable electronic media OR ▪ If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	This requirement is not eligible for the customized approach. (continued on next page)
3.5.1.3	N/A	If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: ▪ Logical access is managed separately and independently of native operating system authentication and access control mechanisms. ▪ Decryption keys are not associated with user accounts. ▪ Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Disk encryption implementations are configured to require independent authentication and logical access controls for decryption.
3.6	N/A	Cryptographic keys used to protect stored account data are secured.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.6.1	N/A	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: ▪ Access to keys is restricted to the fewest number of custodians necessary. ▪ Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ▪ Key-encrypting keys are stored separately from data-encrypting keys. ▪ Keys are stored securely in the fewest possible locations and forms.	Functional	Intersects With	Availability	CRY-08.1	Resiliency mechanisms exist to ensure the availability of data in the event of the loss of cryptographic keys.	5	Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.6.1	N/A	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: ▪ Access to keys is restricted to the fewest number of custodians necessary. ▪ Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ▪ Key-encrypting keys are stored separately from data-encrypting keys. ▪ Keys are stored securely in the fewest possible locations and forms.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.
3.6.1	N/A	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: ▪ Access to keys is restricted to the fewest number of custodians necessary. ▪ Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ▪ Key-encrypting keys are stored separately from data-encrypting keys. ▪ Keys are stored securely in the fewest possible locations and forms.	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	Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.
3.6.1	N/A	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: ▪ Access to keys is restricted to the fewest number of custodians necessary. ▪ Key-encrypting keys are at least as strong as the data-encrypting keys they protect. ▪ Key-encrypting keys are stored separately from data-encrypting keys. ▪ Keys are stored securely in the fewest possible locations and forms.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.
3.6.1.1	N/A	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: ▪ Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. ▪ Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Description of the key usage for each key. ▪ Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	Functional	Intersects With	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	Accurate details of the cryptographic architecture are maintained and available.
3.6.1.1	N/A	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: ▪ Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. ▪ Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Description of the key usage for each key. ▪ Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Accurate details of the cryptographic architecture are maintained and available.
3.6.1.1	N/A	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: ▪ Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. ▪ Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Description of the key usage for each key. ▪ Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	Accurate details of the cryptographic architecture are maintained and available.
3.6.1.2	N/A	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: ▪ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key. ▪ Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. ▪ As at least two full-length key components or key shares, in accordance with an industry-accepted method.	Functional	Intersects With	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access.
3.6.1.2	N/A	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: ▪ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key. ▪ Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. ▪ As at least two full-length key components or key shares, in accordance with an industry-accepted method.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access.
3.6.1.2	N/A	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: ▪ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key. ▪ Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. ▪ As at least two full-length key components or key shares, in accordance with an industry-accepted method.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access.
3.6.1.3	N/A	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Access to cleartext cryptographic key components is restricted to necessary personnel.
3.6.1.4	N/A	Cryptographic keys are stored in the fewest possible locations.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys are retained only where necessary.
3.7	N/A	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.7	N/A	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	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	
3.7.1	N/A	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Strong cryptographic keys are generated.
3.7.1	N/A	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Strong cryptographic keys are generated.
3.7.1	N/A	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	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	Strong cryptographic keys are generated.
3.7.2	N/A	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys are secured during distribution.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.7.2	N/A	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Cryptographic keys are secured during distribution.
3.7.2	N/A	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	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	Cryptographic keys are secured during distribution.
3.7.3	N/A	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys are secured when stored.
3.7.3	N/A	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys are secured when stored.
3.7.3	N/A	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Cryptographic keys are secured when stored.
3.7.3	N/A	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys are secured when stored.
3.7.3	N/A	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	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	Cryptographic keys are secured when stored.
3.7.4	N/A	Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: ▪ A defined cryptoperiod for each key type in use. ▪ A process for key changes at the end of the defined cryptoperiod.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.7.5	N/A	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: ▪ The key has reached the end of its defined cryptoperiod. ▪ The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. ▪ The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
3.7.5	N/A	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: ▪ The key has reached the end of its defined cryptoperiod. ▪ The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. ▪ The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
3.7.5	N/A	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: ▪ The key has reached the end of its defined cryptoperiod. ▪ The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. ▪ The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	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	Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
3.7.5	N/A	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: ▪ The key has reached the end of its defined cryptoperiod. ▪ The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. ▪ The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
3.7.5	N/A	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: ▪ The key has reached the end of its defined cryptoperiod. ▪ The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. ▪ The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	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	Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.
3.7.6	N/A	Where manual cleartext cryptographic key- management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.
3.7.6	N/A	Where manual cleartext cryptographic key- management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.
3.7.6	N/A	Where manual cleartext cryptographic key- management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	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	Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.
3.7.7	N/A	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	Cryptographic keys cannot be substituted by unauthorized personnel.
3.7.7	N/A	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Cryptographic keys cannot be substituted by unauthorized personnel.
3.7.7	N/A	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	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	Cryptographic keys cannot be substituted by unauthorized personnel.
3.7.8	N/A	Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.
3.7.8	N/A	Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.
3.7.8	N/A	Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	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	Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.
3.7.9	N/A	Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	Functional	Intersects With	Third-Party Cryptographic Keys	CRY-09.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.	5	Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.
4.1	N/A	Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	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 (optional)	Notes (optional)
4.1.1	N/A	All security policies and operational procedures that are identified in Requirement 4 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
4.1.1	N/A	All security policies and operational procedures that are identified in Requirement 4 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
4.1.1	N/A	All security policies and operational procedures that are identified in Requirement 4 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 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
4.1.1	N/A	All security policies and operational procedures that are identified in Requirement 4 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 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
4.1.2	N/A	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
4.1.2	N/A	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
4.1.2	N/A	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
4.2	N/A	PAN is protected with strong cryptography during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
4.2.1	N/A	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	N/A	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/regulated 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	N/A	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.
4.2.1.1	N/A	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.
4.2.1.2	N/A	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.1.2	N/A	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.1.2	N/A	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	Cleartext PAN cannot be read or intercepted from wireless network transmissions.
4.2.2	N/A	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/regulated data by end-user messaging technologies.	5	Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.
5.1	N/A	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	Functional	Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
5.1.1	N/A	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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	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	N/A	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 Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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	N/A	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.
5.1.1	N/A	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	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.
5.1.2	N/A	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	Functional	Intersects With	Documented Protection Measures	END-04.2	Mechanisms exist to document antimalware technologies.	5	Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
5.1.2	N/A	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
5.1.2	N/A	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
5.1.2	N/A	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
5.2	N/A	Malicious software (malware) is prevented, or detected and addressed.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
5.2.1	N/A	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
5.2.2	N/A	The deployed anti-malware solution(s): ▪ Detects all known types of malware. ▪ Removes, blocks, or contains all known types of malware.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Malware cannot execute or infect other system components.
5.2.3	N/A	Any system components that are not at risk for malware are evaluated periodically to include the following: ▪ 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	N/A	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	N/A	Anti-malware mechanisms and processes are active, maintained, and monitored.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
5.3	N/A	Anti-malware mechanisms and processes are active, maintained, and monitored.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	
5.3	N/A	Anti-malware mechanisms and processes are active, maintained, and monitored.	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	
5.3.1	N/A	The anti-malware solution(s) is kept current via automatic updates.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Anti-malware mechanisms can detect and address the latest malware threats.
5.3.1	N/A	The anti-malware solution(s) is kept current via automatic updates.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	Anti-malware mechanisms can detect and address the latest malware threats.
5.3.2	N/A	The anti-malware solution(s): ▪ Performs periodic scans and active or real-time scans. OR ▪ Performs continuous behavioral analysis of systems or processes.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Malware cannot complete execution.
5.3.2	N/A	The anti-malware solution(s): ▪ Performs periodic scans and active or real-time scans. OR ▪ Performs continuous behavioral analysis of systems or processes.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Malware cannot complete execution.
5.3.2.1	N/A	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 antimalware 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	N/A	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	N/A	For removable electronic media, the anti- malware solution(s): ▪ 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 antimalware technologies to detect and eradicate malicious code.	5	Malware cannot be introduced to system components via external removable media.
5.3.3	N/A	For removable electronic media, the anti- malware solution(s): ▪ 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	N/A	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Historical records of anti-malware actions are immediately available and retained for at least 12 months.
5.3.4	N/A	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5	Historical records of anti-malware actions are immediately available and retained for at least 12 months.
5.3.5	N/A	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Anti-malware mechanisms cannot be modified by unauthorized personnel.
5.3.5	N/A	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Anti-malware mechanisms cannot be modified by unauthorized personnel.
5.4	N/A	Anti-phishing mechanisms protect users 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	
5.4.1	N/A	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	Functional	Intersects With	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.
6.1	N/A	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
6.1.1	N/A	All security policies and operational procedures that are identified in Requirement 6 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
6.1.1	N/A	All security policies and operational procedures that are identified in Requirement 6 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
6.1.1	N/A	All security policies and operational procedures that are identified in Requirement 6 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 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
6.1.1	N/A	All security policies and operational procedures that are identified in Requirement 6 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 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
6.1.2	N/A	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
6.1.2	N/A	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
6.1.2	N/A	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
6.2	N/A	Bespoke and custom software are developed securely.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
6.2	N/A	Bespoke and custom software are developed securely.	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	
6.2	N/A	Bespoke and custom software are developed securely.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.2	N/A	Bespoke and custom software are developed securely.	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of systems, system components or services 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 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	
6.2	N/A	Bespoke and custom software are developed securely.	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
6.2.1	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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 & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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 systems, system components or services 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 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	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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 Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.1	N/A	Bespoke and custom software are developed securely, as follows: ▪ 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 & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.2	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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 & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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 Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; 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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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 systems, applications and services.	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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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 systems, applications and/or services 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	N/A	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: ▪ 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 & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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 (optional)	Notes (optional)
6.2.3	N/A	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: ▪ Code reviews ensure code is developed according to secure coding guidelines. ▪ Code reviews look for both existing and emerging software vulnerabilities. ▪ Appropriate corrections are implemented prior to release.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Bespoke and custom software cannot be exploited via coding vulnerabilities.
6.2.3	N/A	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: ▪ Code reviews ensure code is developed according to secure coding guidelines. ▪ Code reviews look for both existing and emerging software vulnerabilities. ▪ Appropriate corrections are implemented prior to release.	Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity & data privacy requirements are met and that any identified risks are satisfactorily addressed.	5	Bespoke and custom software cannot be exploited via coding vulnerabilities.
6.2.3	N/A	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: ▪ Code reviews ensure code is developed according to secure coding guidelines. ▪ Code reviews look for both existing and emerging software vulnerabilities. ▪ Appropriate corrections are implemented prior to release.	Functional	Intersects With	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	Bespoke and custom software cannot be exploited via coding vulnerabilities.
6.2.3	N/A	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: ▪ Code reviews ensure code is developed according to secure coding guidelines. ▪ Code reviews look for both existing and emerging software vulnerabilities. ▪ Appropriate corrections are implemented prior to release.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Bespoke and custom software cannot be exploited via coding vulnerabilities.
6.2.3.1	N/A	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: ▪ 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 & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.3.1	N/A	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: ▪ 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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.3.1	N/A	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: ▪ 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 & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.
6.2.4	N/A	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: ▪ 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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	N/A	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: ▪ 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 & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	N/A	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: ▪ 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 Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	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 (optional)	Notes (optional)
6.2.4	N/A	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: ▪ 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 systems, system components or services 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	N/A	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: ▪ 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 systems, system components or services 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.
6.2.4	N/A	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: ▪ 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	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure systems, services and products 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	N/A	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: ▪ 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	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	5	Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.
6.2.4	N/A	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: ▪ 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	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	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 (optional)	Notes (optional)
6.3	N/A	Security vulnerabilities are identified and addressed.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
6.3	N/A	Security vulnerabilities are identified and addressed.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
6.3	N/A	Security vulnerabilities are identified and addressed.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: (1) Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.1	N/A	Security vulnerabilities are identified and managed as follows: ▪ New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). ▪ Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. ▪ Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. ▪ Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	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	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Functional	Intersects With	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.	5	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.
6.3.2	N/A	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.3.3	N/A	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: ▪ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. ▪ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	System components cannot be compromised via the exploitation of a known vulnerability.
6.4	N/A	Public-facing web applications are protected against attacks.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
6.4	N/A	Public-facing web applications are protected against attacks.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	
6.4	N/A	Public-facing web applications are protected against attacks.	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5	
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Public-facing web applications are protected against malicious attacks.
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Public-facing web applications are protected against malicious attacks.
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Public-facing web applications are protected against malicious attacks.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	Public-facing web applications are protected against malicious attacks.
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	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	Public-facing web applications are protected against malicious attacks.
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	Public-facing web applications are protected against malicious attacks.
6.4.1	N/A	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR ▪ Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5	Public-facing web applications are protected against malicious attacks.
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Public-facing web applications are protected in real time against malicious attacks.
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	Public-facing web applications are protected in real time against malicious attacks.
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Public-facing web applications are protected in real time against malicious attacks.
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Public-facing web applications are protected in real time against malicious attacks.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	Public-facing web applications are protected in real time against malicious attacks.
6.4.2	N/A	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: ▪ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. ▪ Actively running and up to date as applicable. ▪ Generating audit logs. ▪ Configured to either block web-based attacks or generate an alert that is immediately investigated.	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5	Public-facing web applications are protected in real time against malicious attacks.
6.4.3	N/A	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: ▪ A method is implemented to confirm that each script is authorized. ▪ A method is implemented to assure the integrity of each script. ▪ An inventory of all scripts is maintained with written justification as to why each is necessary.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.
6.4.3	N/A	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: ▪ A method is implemented to confirm that each script is authorized. ▪ A method is implemented to assure the integrity of each script. ▪ An inventory of all scripts is maintained with written justification as to why each is necessary.	Functional	Intersects With	Unauthorized Code	WEB-01.1	Mechanisms exist to prevent unauthorized code from being present in a secure page as it is rendered in a client's browser.	5	Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.
6.5	N/A	Changes to all system components are managed securely.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
6.5	N/A	Changes to all system components are managed securely.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.5	N/A	Changes to all system components are managed securely.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
6.5	N/A	Changes to all system components are managed securely.	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	
6.5.1	N/A	Changes to all system components in the production environment are made according to established procedures that include: ▪ 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	N/A	Changes to all system components in the production environment are made according to established procedures that include: ▪ 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	N/A	Changes to all system components in the production environment are made according to established procedures that include: ▪ 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	N/A	Changes to all system components in the production environment are made according to established procedures that include: ▪ 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	N/A	Changes to all system components in the production environment are made according to established procedures that include: ▪ 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	N/A	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 maintain a current list of approved technologies (hardware and software).	5	All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.
6.5.2	N/A	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	N/A	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 non-production environment before changes are implemented 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	N/A	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	N/A	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 cybersecurity and/or data privacy 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	N/A	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 cybersecurity & data privacy function 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	N/A	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 vendor-supplied defaults are changed as part of the installation process. 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.
6.5.3	N/A	Pre-production environments are separated from production environments and the separation is enforced with access controls.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	Pre-production environments cannot introduce risks and vulnerabilities into production environments.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.5.3	N/A	Pre-production environments are separated from production environments and the separation is enforced with access controls.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	Pre-production environments cannot introduce risks and vulnerabilities into production environments.
6.5.3	N/A	Pre-production environments are separated from production environments and the separation is enforced with access controls.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	5	Pre-production environments cannot introduce risks and vulnerabilities into production environments.
6.5.4	N/A	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.
6.5.5	N/A	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	Live PANs cannot be present in pre-production environments outside the CDE.
6.5.5	N/A	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	Live PANs cannot be present in pre-production environments outside the CDE.
6.5.5	N/A	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	Functional	Intersects With	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5	Live PANs cannot be present in pre-production environments outside the CDE.
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	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	
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	5	
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge systems, applications and services of test/development/staging data and accounts before it is migrated into a production environment.	5	
6.5.6	N/A	Test data and test accounts are removed from system components before the system goes into production.	Functional	Intersects With	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
7.1	N/A	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
7.1	N/A	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7.1	N/A	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	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	
7.1	N/A	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
7.1	N/A	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	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	
7.1.1	N/A	All security policies and operational procedures that are identified in Requirement 7 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
7.1.1	N/A	All security policies and operational procedures that are identified in Requirement 7 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
7.1.1	N/A	All security policies and operational procedures that are identified in Requirement 7 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 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
7.1.1	N/A	All security policies and operational procedures that are identified in Requirement 7 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 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
7.1.2	N/A	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
7.1.2	N/A	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
7.1.2	N/A	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
7.2	N/A	Access to system components and data is appropriately defined and assigned.	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	
7.2	N/A	Access to system components and data is appropriately defined and assigned.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
7.2	N/A	Access to system components and data is appropriately defined and assigned.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7.2	N/A	Access to system components and data is appropriately defined and assigned.	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	
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Access requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	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	Access requirements are established according to job functions following least-privilege and need-to- know principles.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	Access requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	Access requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	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 requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	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 requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.1	N/A	An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs. ▪ Access to system components and data resources that is based on users' job classification and functions. ▪ The least privileges required (for example, user, administrator) to perform a job function.	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 requirements are established according to job functions following least-privilege and need-to- know principles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: ▪ Job classification and function. ▪ Least privileges necessary to perform job responsibilities.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: ▪ Job classification and function. ▪ Least privileges necessary to perform job responsibilities.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: ▪ Job classification and function. ▪ Least privileges necessary to perform job responsibilities.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.2	N/A	Access is assigned to users, including privileged users, based on: ▪ Job classification and function. ▪ Least privileges necessary to perform job responsibilities.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.
7.2.3	N/A	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	N/A	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	N/A	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 services.	5	Access privileges cannot be granted to users without appropriate, documented authorization.
7.2.3	N/A	Required privileges are approved by authorized personnel.	Functional	Intersects With	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	N/A	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: ▪ 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	N/A	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: ▪ 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	N/A	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	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data 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.
7.2.5	N/A	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	N/A	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	N/A	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 services.	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	N/A	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.
7.2.5.1	N/A	All access by application and system accounts and related access privileges are reviewed as follows: ▪ 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). ▪ The application/system access remains appropriate for the function being performed. ▪ 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	Application and system account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.
7.2.6	N/A	All user access to query repositories of stored cardholder data is restricted as follows: ▪ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. ▪ Only the responsible administrator(s) can directly access or query repositories of stored CHD.	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	Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.
7.2.6	N/A	All user access to query repositories of stored cardholder data is restricted as follows: ▪ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. ▪ Only the responsible administrator(s) can directly access or query repositories of stored CHD.	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	Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
7.2.6	N/A	All user access to query repositories of stored cardholder data is restricted as follows: ▪ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. ▪ Only the responsible administrator(s) can directly access or query repositories of stored CHD.	Functional	Intersects With	Database Access	IAC-20.2	Mechanisms exist to restrict access to databases containing sensitive/regulated data to only necessary services or those individuals whose job requires such access.	5	Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.
7.2.6	N/A	All user access to query repositories of stored cardholder data is restricted as follows: ▪ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. ▪ Only the responsible administrator(s) can directly access or query repositories of stored CHD.	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	Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.
7.2.6	N/A	All user access to query repositories of stored cardholder data is restricted as follows: ▪ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. ▪ Only the responsible administrator(s) can directly access or query repositories of stored CHD.	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.
7.3	N/A	Access to system components and data is managed via an access control system(s).	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7.3	N/A	Access to system components and data is managed via an access control system(s).	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	
7.3	N/A	Access to system components and data is managed via an access control system(s).	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
7.3	N/A	Access to system components and data is managed via an access control system(s).	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	
7.3.1	N/A	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Access rights and privileges are managed via mechanisms intended for that purpose.
7.3.1	N/A	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	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	Access rights and privileges are managed via mechanisms intended for that purpose.
7.3.1	N/A	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	Access rights and privileges are managed via mechanisms intended for that purpose.
7.3.1	N/A	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	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 rights and privileges are managed via mechanisms intended for that purpose.
7.3.2	N/A	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.
7.3.2	N/A	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	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	Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.
7.3.2	N/A	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.
7.3.2	N/A	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	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	Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.
7.3.3	N/A	The access control system(s) is set to "deny all" by default.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Access rights and privileges are prohibited unless expressly permitted.
7.3.3	N/A	The access control system(s) is set to "deny all" by default.	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	Access rights and privileges are prohibited unless expressly permitted.
7.3.3	N/A	The access control system(s) is set to "deny all" by default.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	Access rights and privileges are prohibited unless expressly permitted.
7.3.3	N/A	The access control system(s) is set to "deny all" by default.	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 rights and privileges are prohibited unless expressly permitted.
8.1	N/A	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
8.1	N/A	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	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	
8.1.1	N/A	All security policies and operational procedures that are identified in Requirement 8 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
8.1.1	N/A	All security policies and operational procedures that are identified in Requirement 8 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
8.1.1	N/A	All security policies and operational procedures that are identified in Requirement 8 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
8.1.1	N/A	All security policies and operational procedures that are identified in Requirement 8 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
8.1.2	N/A	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
8.1.2	N/A	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
8.1.2	N/A	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
8.2	N/A	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
8.2	N/A	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	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	
8.2	N/A	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
8.2	N/A	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	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	
8.2.1	N/A	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	All actions by all users are attributable to an individual.
8.2.1	N/A	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	All actions by all users are attributable to an individual.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.2	N/A	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: ▪ Account use is prevented unless needed for an exceptional circumstance. ▪ Use is limited to the time needed for the exceptional circumstance. ▪ Business justification for use is documented. ▪ Use is explicitly approved by management. ▪ Individual user identity is confirmed before access to an account is granted. ▪ Every action taken is attributable to an individual user.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	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 with access to the organization's data or assets.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.3	N/A	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Functional	Intersects With	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5	A service provider's credential used for one customer cannot be used for any other customer.
8.2.4	N/A	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	N/A	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	N/A	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	N/A	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 securely manage authenticators for users and devices.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.4	N/A	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: ▪ Authorized with the appropriate approval. ▪ Implemented with only the privileges specified on the documented approval.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to systems and applications upon termination, as determined by management.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	The accounts of terminated users cannot be used.
8.2.5	N/A	Access for terminated users is immediately revoked.	Functional	Intersects With	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	5	The accounts of terminated users cannot be used.
8.2.6	N/A	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	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.2.7	N/A	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: ▪ Enabled only during the time period needed and disabled when not in use. ▪ Use is monitored for unexpected activity.	Functional	Intersects With	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	Third party remote access cannot be used except where specifically authorized and use is overseen by management.
8.2.8	N/A	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	N/A	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	N/A	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	N/A	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	N/A	Strong authentication for users and administrators is established and managed.	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	N/A	Strong authentication for users and administrators is established and managed.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
8.3	N/A	Strong authentication for users and administrators is established and managed.	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	
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ▪ Something you know, such as a password or passphrase. ▪ Something you have, such as a token device or smart card. ▪ Something you are, such as a biometric element.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ▪ Something you know, such as a password or passphrase. ▪ Something you have, such as a token device or smart card. ▪ Something you are, such as a biometric element.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.1	N/A	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: ▪ Something you know, such as a password or passphrase. ▪ Something you have, such as a token device or smart card. ▪ Something you are, such as a biometric element.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	An account cannot be accessed except with a combination of user identity and an authentication factor.
8.3.2	N/A	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	N/A	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms 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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	User identity is verified before modifying any authentication factor.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
8.3.3	N/A	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	N/A	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	N/A	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	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ▪ Set to a unique value for first-time use and upon reset. ▪ Forced to be changed immediately after the first use.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ▪ Set to a unique value for first-time use and upon reset. ▪ Forced to be changed immediately after the first use.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.5	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: ▪ Set to a unique value for first-time use and upon reset. ▪ Forced to be changed immediately after the first use.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.
8.3.6	N/A	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: ▪ A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). ▪ Contain both numeric and alphabetic characters.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A guessed password/passphrase cannot be verified by either an online or offline brute force attack.
8.3.7	N/A	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.7	N/A	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	A previously used password cannot be used to gain access to an account for at least 12 months.
8.3.8	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.
8.3.8	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/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	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.3.8	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/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	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Functional	Subset Of	Cybersecurity & Data Privacy-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	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate 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	N/A	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 passwords/passphrases. ▪ Instructions to change passwords/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 Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or 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	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ▪ Passwords/passphrases are changed at least once every 90 days, OR ▪ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.3.9	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ▪ Passwords/passphrases are changed at least once every 90 days, OR ▪ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	An undetected compromised password/passphrase cannot be used indefinitely.
8.3.9	N/A	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: ▪ Passwords/passphrases are changed at least once every 90 days, OR ▪ The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	Functional	Intersects With	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.
8.3.10	N/A	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including: ▪ Guidance for customers to change their user passwords/passphrases periodically. ▪ Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	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	Passwords/passphrases for service providers' customers cannot be used indefinitely.
8.3.10	N/A	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including: ▪ Guidance for customers to change their user passwords/passphrases periodically. ▪ Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	Passwords/passphrases for service providers' customers cannot be used indefinitely.
8.3.10.1	N/A	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer 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 securely manage authenticators for users and devices.	5	Passwords/passphrases for service providers' customers cannot be used indefinitely.
8.3.10.1	N/A	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer 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	Passwords/passphrases for service providers' customers cannot be used indefinitely.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	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 authentication factor cannot be used by anyone other than the user to which it is assigned.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	An authentication factor cannot be used by anyone other than the user to which it is assigned.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	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	An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.3.11	N/A	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: ▪ Factors are assigned to an individual user and not shared among multiple users. ▪ Physical and/or logical controls ensure only the intended user can use that factor to gain access.	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	An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.4	N/A	Multi-factor authentication (MFA) is implemented to secure 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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
8.4.1	N/A	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	Administrative access to the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	N/A	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Access into the CDE cannot be obtained by the use of a single authentication factor.
8.4.2	N/A	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	N/A	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	N/A	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.
8.4.2	N/A	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	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ▪ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ▪ All remote access by third parties and vendors.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.4.3	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ▪ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ▪ All remote access by third parties and vendors.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.4.3	N/A	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: ▪ All remote access by all personnel, both users and administrators, originating from outside the entity's network. ▪ All remote access by third parties and vendors.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	Remote access to the entity's network cannot be obtained by using a single authentication factor.
8.5	N/A	Multi-factor authentication (MFA) systems are configured to prevent misuse.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
8.5	N/A	Multi-factor authentication (MFA) systems are configured to prevent misuse.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
8.5	N/A	Multi-factor authentication (MFA) systems are configured to prevent misuse.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
8.5	N/A	Multi-factor authentication (MFA) systems are configured to prevent misuse.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
8.5.1	N/A	MFA systems are implemented as follows: ▪ 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	N/A	MFA systems are implemented as follows: ▪ 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	N/A	MFA systems are implemented as follows: ▪ 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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	MFA systems are resistant to attack and strictly control any administrative overrides.
8.5.1	N/A	MFA systems are implemented as follows: ▪ 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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	MFA systems are resistant to attack and strictly control any administrative overrides.
8.6	N/A	Use of application and system accounts and associated authentication factors is strictly managed.	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	
8.6	N/A	Use of application and system accounts and associated authentication factors is strictly managed.	Functional	Intersects With	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
8.6	N/A	Use of application and system accounts and associated authentication factors is strictly managed.	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	
8.6	N/A	Use of application and system accounts and associated authentication factors is strictly managed.	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	
8.6.1	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.6.1	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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 with access to the organization's data or assets.	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	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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 account 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	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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	N/A	If accounts used by systems or applications can be used for interactive login, they are managed as follows: ▪ 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	N/A	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	N/A	Passwords/passphrases for any application and system accounts are protected against misuse as follows: ▪ 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 passwords/passphrases.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	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	N/A	Passwords/passphrases for any application and system accounts are protected against misuse as follows: ▪ 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 passwords/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	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	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	
9.1	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	
9.1	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
9.1	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	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	
9.1	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	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	
9.1	N/A	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	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) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.1.1	N/A	All security policies and operational procedures that are identified in Requirement 9 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.2	N/A	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
9.1.2	N/A	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
9.1.2	N/A	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
9.1.2	N/A	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	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) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
9.2	N/A	Physical access controls manage entry into facilities and systems containing cardholder data.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
9.2	N/A	Physical access controls manage entry into facilities and systems containing cardholder data.	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	
9.2	N/A	Physical access controls manage entry into facilities and systems containing cardholder data.	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	
9.2	N/A	Physical access controls manage entry into facilities and systems containing cardholder data.	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) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
9.2	N/A	Physical access controls manage entry into facilities and systems containing cardholder data.	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	
9.2.1	N/A	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Physical Access Authorizations	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	N/A	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Role-Based Physical Access	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	N/A	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) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1	N/A	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Functional	Intersects With	Controlled Ingress & Egress Points	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	N/A	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	N/A	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: ▪ 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	N/A	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: ▪ 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	N/A	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: ▪ 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	N/A	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: ▪ 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 Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information 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	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.2.2	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.2.2	N/A	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	Unauthorized devices cannot connect to the entity's network from public areas within the facility.
9.2.3	N/A	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	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	Physical networking equipment cannot be accessed by unauthorized personnel.
9.2.3	N/A	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	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	Physical networking equipment cannot be accessed by unauthorized personnel.
9.2.3	N/A	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	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	Physical networking equipment cannot be accessed by unauthorized personnel.
9.2.4	N/A	Access to consoles in sensitive areas is restricted via locking when not in use.	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	Physical consoles within sensitive areas cannot be used by unauthorized personnel.
9.2.4	N/A	Access to consoles in sensitive areas is restricted via locking when not in use.	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	5	Physical consoles within sensitive areas cannot be used by unauthorized personnel.
9.3	N/A	Physical access for personnel and visitors is authorized and managed.	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	
9.3	N/A	Physical access for personnel and visitors is authorized and managed.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.3	N/A	Physical access for personnel and visitors is authorized and managed.	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	
9.3.1	N/A	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: ▪ Identifying personnel. ▪ Managing changes to an individual's physical access requirements. ▪ Revoking or terminating personnel identification. ▪ Limiting access to the identification process or system to authorized personnel.	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	Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.
9.3.1	N/A	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: ▪ Identifying personnel. ▪ Managing changes to an individual's physical access requirements. ▪ Revoking or terminating personnel identification. ▪ Limiting access to the identification process or system to authorized personnel.	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	Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.
9.3.1	N/A	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: ▪ Identifying personnel. ▪ Managing changes to an individual's physical access requirements. ▪ Revoking or terminating personnel identification. ▪ Limiting access to the identification process or system to authorized personnel.	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	Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.
9.3.1.1	N/A	Physical access to sensitive areas within the CDE for personnel is controlled as follows: ▪ Access is authorized and based on individual job function. ▪ Access is revoked immediately upon termination. ▪ All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	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	Sensitive areas cannot be accessed by unauthorized personnel.
9.3.1.1	N/A	Physical access to sensitive areas within the CDE for personnel is controlled as follows: ▪ Access is authorized and based on individual job function. ▪ Access is revoked immediately upon termination. ▪ All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	Sensitive areas cannot be accessed by unauthorized personnel.
9.3.1.1	N/A	Physical access to sensitive areas within the CDE for personnel is controlled as follows: ▪ Access is authorized and based on individual job function. ▪ Access is revoked immediately upon termination. ▪ All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	Sensitive areas cannot be accessed by unauthorized personnel.
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	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	
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	Functional	Intersects With	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	5	Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	Functional	Intersects With	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one (1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	5	Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.
9.3.2	N/A	Procedures are implemented for authorizing and managing visitor access to the CDE, including: ▪ Visitors are authorized before entering. ▪ Visitors are escorted at all times. ▪ Visitors are clearly identified and given a badge or other identification that expires. ▪ Visitor badges or other identification visibly distinguishes visitors from personnel.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.
9.3.3	N/A	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	Visitor identification or badges cannot be reused after expiration.
9.3.3	N/A	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Functional	Intersects With	Visitor Access Revocation	PES-06.6	Mechanisms exist to ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.	5	Visitor identification or badges cannot be reused after expiration.
9.3.4	N/A	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: ▪ The visitor's name and the organization represented. ▪ The date and time of the visit. ▪ The name of the personnel authorizing physical access. ▪ Retaining the log for at least three months, unless otherwise restricted by law.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	Records of visitor access that enable the identification of individuals are maintained.
9.3.4	N/A	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: ▪ The visitor's name and the organization represented. ▪ The date and time of the visit. ▪ The name of the personnel authorizing physical access. ▪ Retaining the log for at least three months, unless otherwise restricted by law.	Functional	Intersects With	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.	5	Records of visitor access that enable the identification of individuals are maintained.
9.3.4	N/A	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: ▪ The visitor's name and the organization represented. ▪ The date and time of the visit. ▪ The name of the personnel authorizing physical access. ▪ Retaining the log for at least three months, unless otherwise restricted by law.	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	Records of visitor access that enable the identification of individuals are maintained.
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	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	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Functional	Intersects With	Storage Media	CRY-05.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive/regulated data residing on storage media.	5	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	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	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Functional	Intersects With	Making Sensitive Data Unreadable In Storage	DCH-06.4	Mechanisms exist to ensure sensitive/regulated data is rendered human unreadable anywhere sensitive/regulated data is stored.	5	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	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	
9.4	N/A	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	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	
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1	N/A	All media with cardholder data is physically secured.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.1.1	N/A	Offline media backups with cardholder data are stored in a secure location.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	Offline backups cannot be accessed by unauthorized personnel.
9.4.1.2	N/A	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Functional	Intersects With	Data Storage Location Reviews	BCD-02.4	Mechanisms exist to perform periodic security reviews of storage locations that contain sensitive / regulated data.	5	The security controls protecting offline backups are verified periodically by inspection.
9.4.1.2	N/A	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	The security controls protecting offline backups are verified periodically by inspection.
9.4.1.2	N/A	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	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	The security controls protecting offline backups are verified periodically by inspection.
9.4.1.2	N/A	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	The security controls protecting offline backups are verified periodically by inspection.
9.4.1.2	N/A	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	The security controls protecting offline backups are verified periodically by inspection.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	Media are classified and protected appropriately.
9.4.2	N/A	All media with cardholder data is classified in accordance with the sensitivity of the data.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	Media are classified and protected appropriately.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ▪ Media sent outside the facility is logged. ▪ Media is sent by secured courier or other delivery method that can be accurately tracked. ▪ Offsite tracking logs include details about media location.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	Media is secured and tracked when transported outside the facility.
9.4.3	N/A	Media with cardholder data sent outside the facility is secured as follows: ▪ Media sent outside the facility is logged. ▪ Media is sent by secured courier or other delivery method that can be accurately tracked. ▪ Offsite tracking logs include details about media location.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	Media is secured and tracked when transported outside the facility.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.4	N/A	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Functional	Intersects With	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive / regulated media that is transferred outside of the organization's facilities.	5	Media cannot leave a facility without the approval of accountable personnel.
9.4.5	N/A	Inventory logs of all electronic media with cardholder data are maintained.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	Accurate inventories of stored electronic media are maintained.
9.4.5.1	N/A	Inventories of electronic media with cardholder data are conducted at least once every 12 months.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	Media inventories are verified periodically.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ▪ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ▪ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ▪ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ▪ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.6	N/A	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: ▪ Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. ▪ Materials are stored in secure storage containers prior to destruction.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.7	N/A	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ▪ The electronic media is destroyed. ▪ The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	Cardholder data cannot be recovered from media that has been erased or destroyed.
9.4.7	N/A	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ▪ The electronic media is destroyed. ▪ The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Cardholder data cannot be recovered from media that has been erased or destroyed.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.4.7	N/A	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ▪ The electronic media is destroyed. ▪ The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	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 erased or destroyed.
9.4.7	N/A	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ▪ The electronic media is destroyed. ▪ The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	Cardholder data cannot be recovered from media that has been erased or destroyed.
9.4.7	N/A	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ▪ The electronic media is destroyed. ▪ The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	Cardholder data cannot be recovered from media that has been erased or destroyed.
9.5	N/A	Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.	5	
9.5	N/A	Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Inspection of Systems, Components & Devices	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1	N/A	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: ▪ Maintaining a list of POI devices. ▪ Periodically inspecting POI devices to look for tampering or unauthorized substitution. ▪ Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	The identity and location of POI devices is recorded and known at all times.
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	The identity and location of POI devices is recorded and known at all times.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.5.1.1	N/A	An up-to-date list of POI devices is maintained, including: ▪ Make and model of the device. ▪ Location of device. ▪ Device serial number or other methods of unique identification.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	The identity and location of POI devices is recorded and known at all times.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.
9.5.1.2	N/A	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Functional	Intersects With	Inspection of Systems, Components & Devices	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.
9.5.1.2.1	N/A	The frequency of periodic POI device inspections and the type of inspections performed 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	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	POI devices are inspected at a frequency that addresses the entity's risk.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.
9.5.1.3	N/A	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: ▪ Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. ▪ Procedures to ensure devices are not installed, replaced, or returned without verification. ▪ Being aware of suspicious behavior around devices. ▪ Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy 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	N/A	Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
10.1.1	N/A	All security policies and operational procedures that are identified in Requirement 10 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	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	N/A	All security policies and operational procedures that are identified in Requirement 10 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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	N/A	All security policies and operational procedures that are identified in Requirement 10 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 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	N/A	All security policies and operational procedures that are identified in Requirement 10 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 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
10.1.2	N/A	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
10.1.2	N/A	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
10.1.2	N/A	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	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 (optional)	Notes (optional)
10.2	N/A	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.	5	
10.2.1	N/A	Audit logs are enabled and active for all system components and cardholder data.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all activities affecting system components and cardholder data are captured.
10.2.1	N/A	Audit logs are enabled and active for all system components and cardholder data.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all activities affecting system components and cardholder data are captured.
10.2.1	N/A	Audit logs are enabled and active for all system components and cardholder data.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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 activities affecting system components and cardholder data are captured.
10.2.1	N/A	Audit logs are enabled and active for all system components and cardholder data.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all activities affecting system components and cardholder data are captured.
10.2.1.1	N/A	Audit logs capture all individual user access to cardholder data.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all individual user access to cardholder data are captured.
10.2.1.1	N/A	Audit logs capture all individual user access to cardholder data.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all individual user access to cardholder data are captured.
10.2.1.1	N/A	Audit logs capture all individual user access to cardholder data.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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 individual user access to cardholder data are captured.
10.2.1.1	N/A	Audit logs capture all individual user access to cardholder data.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all individual user access to cardholder data are captured.
10.2.1.1	N/A	Audit logs capture all individual user access to cardholder data.	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 individual user access to cardholder data are captured.
10.2.1.2	N/A	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms 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	N/A	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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems 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	N/A	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-21.4	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	N/A	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 systems 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	N/A	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	N/A	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.
10.2.1.3	N/A	Audit logs capture all access to audit logs.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all access to audit logs are captured.
10.2.1.3	N/A	Audit logs capture all access to audit logs.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all access to audit logs are captured.
10.2.1.3	N/A	Audit logs capture all access to audit logs.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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 access to audit logs are captured.
10.2.1.3	N/A	Audit logs capture all access to audit logs.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of all access to audit logs are captured.
10.2.1.3	N/A	Audit logs capture all access to audit logs.	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 access to audit logs are captured.
10.2.1.4	N/A	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all invalid access attempts are captured.
10.2.1.4	N/A	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all invalid access attempts are captured.
10.2.1.4	N/A	Audit logs capture all invalid logical access attempts.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	N/A	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	N/A	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	N/A	Audit logs capture all changes to identification and authentication credentials including, but not limited to: ▪ 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 systems 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	N/A	Audit logs capture all changes to identification and authentication credentials including, but not limited to: ▪ 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	N/A	Audit logs capture all changes to identification and authentication credentials including, but not limited to: ▪ 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	N/A	Audit logs capture all changes to identification and authentication credentials including, but not limited to: ▪ Creation of new accounts. ▪ Elevation of privileges. ▪ All changes, additions, or deletions to accounts with administrative access.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all changes to identification and authentication credentials are captured.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.2.1.5	N/A	Audit logs capture all changes to identification and authentication credentials including, but not limited to: ▪ Creation of new accounts. ▪ Elevation of privileges. ▪ All changes, additions, or deletions to accounts with administrative access.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all changes to identification and authentication credentials are captured.
10.2.1.6	N/A	Audit logs capture the following: ▪ All initialization of new audit logs, and ▪ All starting, stopping, or pausing of the existing audit logs.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of all changes to audit log activity status are captured.
10.2.1.6	N/A	Audit logs capture the following: ▪ All initialization of new audit logs, and ▪ All starting, stopping, or pausing of the existing audit logs.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of all changes to audit log activity status are captured.
10.2.1.6	N/A	Audit logs capture the following: ▪ All initialization of new audit logs, and ▪ All starting, stopping, or pausing of the existing audit logs.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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 audit log activity status are captured.
10.2.1.6	N/A	Audit logs capture the following: ▪ All initialization of new audit logs, and ▪ All starting, stopping, or pausing of the existing audit logs.	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 audit log activity status are captured.
10.2.1.6	N/A	Audit logs capture the following: ▪ All initialization of new audit logs, and ▪ All starting, stopping, or pausing of the existing audit logs.	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 audit log activity status are captured.
10.2.1.7	N/A	Audit logs capture all creation and deletion of system-level objects.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Records of alterations that indicate a system has been modified from its intended functionality are captured.
10.2.1.7	N/A	Audit logs capture all creation and deletion of system-level objects.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Records of alterations that indicate a system has been modified from its intended functionality are captured.
10.2.1.7	N/A	Audit logs capture all creation and deletion of system-level objects.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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 alterations that indicate a system has been modified from its intended functionality are captured.
10.2.1.7	N/A	Audit logs capture all creation and deletion of system-level objects.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	Records of alterations that indicate a system has been modified from its intended functionality are captured.
10.2.1.7	N/A	Audit logs capture all creation and deletion of system-level objects.	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 alterations that indicate a system has been modified from its intended functionality are captured.
10.2.2	N/A	Audit logs record the following details for each auditable event: ▪ User identification. ▪ Type of event. ▪ Date and time. ▪ Success and failure indication. ▪ Origination of event. ▪ Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms 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 10.2.1 are captured.
10.2.2	N/A	Audit logs record the following details for each auditable event: ▪ User identification. ▪ Type of event. ▪ Date and time. ▪ Success and failure indication. ▪ Origination of event. ▪ Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems 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 10.2.1 are captured.
10.2.2	N/A	Audit logs record the following details for each auditable event: ▪ User identification. ▪ Type of event. ▪ Date and time. ▪ Success and failure indication. ▪ Origination 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 systems 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 10.2.1 are captured.
10.2.2	N/A	Audit logs record the following details for each auditable event: ▪ User identification. ▪ Type of event. ▪ Date and time. ▪ Success and failure indication. ▪ Origination 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 10.2.1 are captured.
10.3	N/A	Audit logs are protected from destruction and unauthorized modifications.	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	
10.3	N/A	Audit logs are protected from destruction and unauthorized modifications.	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	
10.3.1	N/A	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	N/A	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.
10.3.2	N/A	Audit log 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	N/A	Audit log 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	N/A	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	N/A	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	N/A	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	N/A	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 selected files and configuration settings.	5	Stored activity records cannot be modified without an alert being generated.
10.3.4	N/A	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 assets to generate alerts for unauthorized modifications.	5	Stored activity records cannot be modified without an alert being generated.
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	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	
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	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 assets to generate alerts for unauthorized modifications.	5	
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	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	
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	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	
10.4	N/A	Audit logs are reviewed to identify anomalies or suspicious activity.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	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 (optional)	Notes (optional)
10.4.1	N/A	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 SAD. ▪ 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	N/A	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 SAD. ▪ 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 privacy and supply chain activities to achieve integrated situational awareness.	5	Potentially suspicious or anomalous activities are quickly identified to minimize impact.
10.4.1	N/A	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 SAD. ▪ 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	N/A	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 SAD. ▪ 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.
10.4.1	N/A	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 SAD. ▪ 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	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	N/A	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	N/A	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 privacy 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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	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 privacy and supply chain activities to achieve integrated situational awareness.	5	Suspicious or anomalous activities are addressed.
10.4.3	N/A	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	N/A	Audit log history is retained and 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	N/A	Audit log history is retained and 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	N/A	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	N/A	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	N/A	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	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	Historical records of activity are available immediately to support incident response and are retained for at least 12 months.
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	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	
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.	5	
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
10.6	N/A	Time-synchronization mechanisms support consistent time settings across all systems.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
10.6.1	N/A	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Common time is established across all systems.
10.6.1	N/A	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Common time is established across all systems.
10.6.1	N/A	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	N/A	System clocks and time are synchronized using time-synchronization technology.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.	5	Common time is established across all systems.
10.6.1	N/A	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	N/A	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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.6.2	N/A	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 Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	The time on all systems is accurate and consistent.
10.6.2	N/A	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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	The time on all systems is accurate and consistent.
10.6.2	N/A	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	N/A	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 systems 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	N/A	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	N/A	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	N/A	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 Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	N/A	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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	N/A	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	N/A	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 systems to use an authoritative time source to generate time stamps for event logs.	5	System time settings cannot be modified by unauthorized personnel.
10.6.3	N/A	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	N/A	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.
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s).	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	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 (optional)	Notes (optional)
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO).	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
10.7	N/A	Failures of critical security control systems are detected, reported, and responded to promptly.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	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	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	Failures in critical security control systems are promptly identified and addressed.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.1	N/A	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ FIM. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used).	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	Failures in critical security control systems are promptly identified and addressed.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.2	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: ▪ Network security controls. ▪ IDS/IPS. ▪ Change-detection mechanisms. ▪ Anti-malware solutions. ▪ Physical access controls. ▪ Logical access controls. ▪ Audit logging mechanisms. ▪ Segmentation controls (if used). ▪ Audit log review mechanisms. ▪ Automated security testing tools (if used).	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	Failures in critical security control systems are promptly identified and addressed.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
10.7.3	N/A	Failures of any critical security controls systems are responded to promptly, including but not limited to: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure and documenting required remediation. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.
11.1	N/A	Processes and mechanisms for regularly testing security of systems and networks are defined and understood.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
11.1	N/A	Processes and mechanisms for regularly testing security of systems and networks are defined and understood.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
11.1.1	N/A	All security policies and operational procedures that are identified in Requirement 11 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 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
11.1.1	N/A	All security policies and operational procedures that are identified in Requirement 11 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 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
11.1.1	N/A	All security policies and operational procedures that are identified in Requirement 11 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Expectations, controls, and oversight for meeting activities within Requirement 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
11.1.1	N/A	All security policies and operational procedures that are identified in Requirement 11 are: ▪ Documented. ▪ Kept up to date. ▪ In use. ▪ Known to all affected parties.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, 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 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
11.1.2	N/A	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
11.1.2	N/A	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	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	Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
11.1.2	N/A	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	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	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Wireless Intrusion Detection System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS)	NET-08.2	Mechanisms exist to monitor wireless network segments to implement Wireless Intrusion Detection / Prevention Systems (WIDS/WIPS) technologies.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	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	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
11.2	N/A	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	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	
11.2.1	N/A	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	N/A	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	N/A	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 systems.	5	Unauthorized wireless access points are identified and addressed periodically.
11.2.1	N/A	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	N/A	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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.2.1	N/A	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	N/A	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	N/A	An inventory of authorized wireless access points is maintained, including a documented business justification.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	Unauthorized wireless access points are not mistaken for authorized wireless access points.
11.2.2	N/A	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	N/A	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	N/A	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	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
11.3	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
11.3	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	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	
11.3	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	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	
11.3	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
11.3	N/A	External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Functional	Intersects With	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO).	5	
11.3.1	N/A	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-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified 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	N/A	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	N/A	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	N/A	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	N/A	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	N/A	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)
11.3.1.1	N/A	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: ▪ Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ▪ Rescans are conducted as needed.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	Lower ranked vulnerabilities (lower than high or critical) are addressed at a frequency in accordance with the entity's risk.
11.3.1.1	N/A	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: ▪ Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ▪ Rescans are conducted as needed.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	Lower ranked vulnerabilities (lower than high or critical) are addressed at a frequency in accordance with the entity's risk.
11.3.1.1	N/A	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: ▪ Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ▪ Rescans are conducted as needed.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	Lower ranked vulnerabilities (lower than high or critical) are addressed at a frequency in accordance with the entity's risk.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.3.1.2	N/A	Internal vulnerability scans are performed via authenticated scanning as follows: ▪ Systems that are unable to accept credentials for authenticated scanning are documented. ▪ Sufficient privileges are used for those systems that accept credentials for scanning. ▪ If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.
11.3.1.2	N/A	Internal vulnerability scans are performed via authenticated scanning as follows: ▪ Systems that are unable to accept credentials for authenticated scanning are documented. ▪ Sufficient privileges are used for those systems that accept credentials for scanning. ▪ If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.
11.3.1.2	N/A	Internal vulnerability scans are performed via authenticated scanning as follows: ▪ Systems that are unable to accept credentials for authenticated scanning are documented. ▪ Sufficient privileges are used for those systems that accept credentials for scanning. ▪ If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.
11.3.1.2	N/A	Internal vulnerability scans are performed via authenticated scanning as follows: ▪ Systems that are unable to accept credentials for authenticated scanning are documented. ▪ Sufficient privileges are used for those systems that accept credentials for scanning. ▪ If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	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	Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.
11.3.1.3	N/A	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 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 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	N/A	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 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 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	N/A	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 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 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	N/A	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 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	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	This requirement is not eligible for the customized approach.
11.3.2	N/A	External vulnerability scans are performed as follows: ▪ At least once every three months. ▪ By a PCI SSC Approved Scanning Vendor (ASV). ▪ Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. ▪ Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	This requirement is not eligible for the customized approach.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ▪ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ▪ Rescans are conducted as needed. ▪ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ▪ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ▪ Rescans are conducted as needed. ▪ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ▪ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ▪ Rescans are conducted as needed. ▪ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ▪ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ▪ Rescans are conducted as needed. ▪ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.3.2.1	N/A	External vulnerability scans are performed after any significant change as follows: ▪ Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. ▪ Rescans are conducted as needed. ▪ Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.
11.4	N/A	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
11.4.1	N/A	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: ▪ Industry-accepted penetration testing approaches. ▪ Coverage for the entire CDE perimeter and critical systems. ▪ Testing from both inside and outside the network. ▪ Testing to validate any segmentation and scope- reduction controls. ▪ Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. ▪ Network-layer penetration tests that encompass all components that support network functions as well as operating systems. ▪ Review and consideration of threats and vulnerabilities experienced in the last 12 months. ▪ Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▪ Retention of penetration testing results and remediation activities results for at least 12 months.	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	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.
11.4.1	N/A	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: ▪ Industry-accepted penetration testing approaches. ▪ Coverage for the entire CDE perimeter and critical systems. ▪ Testing from both inside and outside the network. ▪ Testing to validate any segmentation and scope- reduction controls. ▪ Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. ▪ Network-layer penetration tests that encompass all components that support network functions as well as operating systems. ▪ Review and consideration of threats and vulnerabilities experienced in the last 12 months. ▪ Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▪ Retention of penetration testing results and remediation activities results for at least 12 months.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.
11.4.1	N/A	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: ▪ Industry-accepted penetration testing approaches. ▪ Coverage for the entire CDE perimeter and critical systems. ▪ Testing from both inside and outside the network. ▪ Testing to validate any segmentation and scope- reduction controls. ▪ Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. ▪ Network-layer penetration tests that encompass all components that support network functions as well as operating systems. ▪ Review and consideration of threats and vulnerabilities experienced in the last 12 months. ▪ Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▪ Retention of penetration testing results and remediation activities results for at least 12 months.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.
11.4.1	N/A	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: ▪ Industry-accepted penetration testing approaches. ▪ Coverage for the entire CDE perimeter and critical systems. ▪ Testing from both inside and outside the network. ▪ Testing to validate any segmentation and scope- reduction controls. ▪ Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. ▪ Network-layer penetration tests that encompass all components that support network functions as well as operating systems. ▪ Review and consideration of threats and vulnerabilities experienced in the last 12 months. ▪ Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▪ Retention of penetration testing results and remediation activities results for at least 12 months.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.
11.4.1	N/A	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: ▪ Industry-accepted penetration testing approaches. ▪ Coverage for the entire CDE perimeter and critical systems. ▪ Testing from both inside and outside the network. ▪ Testing to validate any segmentation and scope- reduction controls. ▪ Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. ▪ Network-layer penetration tests that encompass all components that support network functions as well as operating systems. ▪ Review and consideration of threats and vulnerabilities experienced in the last 12 months. ▪ Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▪ Retention of penetration testing results and remediation activities results for at least 12 months.	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	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.
11.4.2	N/A	Internal penetration testing is performed: ▪ Per the entity's defined methodology, ▪ At least once every 12 months ▪ After any significant infrastructure or application upgrade or change ▪ 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 systems and web applications.	5	Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.
11.4.2	N/A	Internal penetration testing is performed: ▪ Per the entity's defined methodology, ▪ At least once every 12 months ▪ After any significant infrastructure or application upgrade or change ▪ 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	Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.
11.4.3	N/A	External penetration testing is performed: ▪ Per the entity's defined methodology ▪ At least once every 12 months ▪ After any significant infrastructure or application upgrade or change ▪ By a qualified internal resource or qualified external third party ▪ Organizational independence of the tester exists (not required to be a QSA or ASV). (continued on next page)	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	External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown 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 (optional)	Notes (optional)
11.4.3	N/A	External penetration testing is performed: ▪ Per the entity's defined methodology ▪ At least once every 12 months ▪ After any significant infrastructure or application upgrade or change ▪ By a qualified internal resource or qualified external third party ▪ Organizational independence of the tester exists (not required to be a QSA or ASV). (continued on next page)	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.
11.4.4	N/A	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: ▪ In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. ▪ Penetration testing is repeated to verify the corrections.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.
11.4.4	N/A	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: ▪ In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. ▪ Penetration testing is repeated to verify the corrections.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.
11.4.4	N/A	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: ▪ In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. ▪ Penetration testing is repeated to verify the corrections.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.4.5	N/A	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every 12 months and after any changes to segmentation controls/methods ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six 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 by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six months and after any changes to segmentation controls/methods. ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six months and after any changes to segmentation controls/methods. ▪ Covering all segmentation controls/methods in use. ▪ According to the entity's defined penetration testing methodology. ▪ Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. ▪ Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). ▪ Performed by a qualified internal resource or qualified external third party. ▪ Organizational independence of the tester exists (not required to be a QSA or ASV).	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six 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 by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six 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	If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six 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 systems and web applications.	5	If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.4.6	N/A	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: ▪ At least once every six 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 by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.
11.4.7	N/A	Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5	N/A	Network intrusions and unexpected file changes are detected and responded to.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5	N/A	Network intrusions and unexpected file changes are detected and responded to.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5	N/A	Network intrusions and unexpected file changes are detected and responded to.	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 assets to generate alerts for unauthorized modifications.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5	N/A	Network intrusions and unexpected file changes are detected and responded to.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5	N/A	Network intrusions and unexpected file changes are detected and responded to.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.
11.5.1	N/A	Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: ▪ All traffic is monitored at the perimeter of the CDE. ▪ All traffic is monitored at critical points in the CDE. ▪ Personnel are alerted to suspected compromises. ▪ All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.
11.5.1	N/A	Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: ▪ All traffic is monitored at the perimeter of the CDE. ▪ All traffic is monitored at critical points in the CDE. ▪ Personnel are alerted to suspected compromises. ▪ All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	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	Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.
11.5.1	N/A	Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: ▪ All traffic is monitored at the perimeter of the CDE. ▪ All traffic is monitored at critical points in the CDE. ▪ Personnel are alerted to suspected compromises. ▪ All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.
11.5.1	N/A	Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: ▪ All traffic is monitored at the perimeter of the CDE. ▪ All traffic is monitored at critical points in the CDE. ▪ Personnel are alerted to suspected compromises. ▪ All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.
11.5.1.1	N/A	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.
11.5.1.1	N/A	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Functional	Intersects With	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5	Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.
11.5.1.1	N/A	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Functional	Intersects With	Covert Channel Analysis	MON-15	Mechanisms exist to conduct covert channel analysis to identify aspects of communications that are potential avenues for covert channels.	5	Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.
11.5.1.1	N/A	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.
11.5.1.1	N/A	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.
11.5.2	N/A	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: ▪ 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 files and configuration settings.	5	Critical files cannot be modified by unauthorized personnel without an alert being generated.
11.5.2	N/A	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: ▪ 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-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	5	Critical files cannot be modified by unauthorized personnel without an alert being generated.
11.6	N/A	Unauthorized changes on payment pages are detected and responded to.	Functional	Intersects With	Website Change Detection	WEB-13	Mechanisms exist to detect and respond to Indicators of Compromise (IoC) for unauthorized alterations, additions, deletions or changes on websites that store, process and/or transmit sensitive / regulated data.	5	
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
11.6.1	N/A	A change- and tamper-detection mechanism is deployed as follows: ▪ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. ▪ The mechanism is configured to evaluate the received HTTP header and payment page. ▪ The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Functional	Intersects With	Website Change Detection	WEB-13	Mechanisms exist to detect and respond to Indicators of Compromise (IoC) for unauthorized alterations, additions, deletions or changes on websites that store, process and/or transmit sensitive / regulated data.	5	E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.
12.1	N/A	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
12.1	N/A	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
12.1.1	N/A	An overall information security policy is: ▪ Established. ▪ Published. ▪ Maintained. ▪ Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	The strategic objectives and principles of information security are defined, adopted, and known to all personnel.
12.1.1	N/A	An overall information security policy is: ▪ Established. ▪ Published. ▪ Maintained. ▪ Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	The strategic objectives and principles of information security are defined, adopted, and known to all personnel.
12.1.2	N/A	The information security policy is: ▪ Reviewed at least once every 12 months. ▪ Updated as needed to reflect changes to business objectives or risks to the environment.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	The information security policy continues to reflect the organization's strategic objectives and principles.
12.1.2	N/A	The information security policy is: ▪ Reviewed at least once every 12 months. ▪ Updated as needed to reflect changes to business objectives or risks to the environment.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	The information security policy continues to reflect the organization's strategic objectives and principles.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.3	N/A	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	Personnel understand their role in protecting the entity's cardholder data.
12.1.4	N/A	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	A designated member of executive management is responsible for information security.
12.1.4	N/A	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	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 designated member of executive management is responsible for information security.
12.2	N/A	Acceptable use policies for end-user technologies are defined and implemented.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
12.2	N/A	Acceptable use policies for end-user technologies are defined and implemented.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	
12.2	N/A	Acceptable use policies for end-user technologies are defined and implemented.	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	
12.2	N/A	Acceptable use policies for end-user technologies are defined and implemented.	Functional	Intersects With	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
12.2.1	N/A	Acceptable use policies for end-user technologies are documented and implemented, including: ▪ 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	N/A	Acceptable use policies for end-user technologies are documented and implemented, including: ▪ 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 & data privacy principles in their daily work.	5	The use of end-user technologies is defined and managed to ensure authorized usage.
12.2.1	N/A	Acceptable use policies for end-user technologies are documented and implemented, including: ▪ 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	N/A	Acceptable use policies for end-user technologies are documented and implemented, including: ▪ 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	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	The use of end-user technologies is defined and managed to ensure authorized usage.
12.3	N/A	Risks to the cardholder data environment are formally identified, evaluated, and managed.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
12.3	N/A	Risks to the cardholder data environment are formally identified, evaluated, and managed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
12.3	N/A	Risks to the cardholder data environment are formally identified, evaluated, and managed.	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 systems and data.	5	
12.3	N/A	Risks to the cardholder data environment are formally identified, evaluated, and managed.	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	
12.3	N/A	Risks to the cardholder data environment are formally identified, evaluated, and managed.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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 (optional)	Notes (optional)
12.3.1	N/A	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: ▪ 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	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	N/A	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: ▪ 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 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	N/A	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: ▪ 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 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	N/A	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: ▪ 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	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 systems and data.	5	Up to date knowledge and assessment of risks to the CDE are maintained.
12.3.1	N/A	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: ▪ 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	N/A	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: ▪ 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	N/A	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: ▪ 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.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.3.1	N/A	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: ▪ 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	N/A	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: ▪ 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.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	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	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	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 systems and data.	5	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.2	N/A	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: ▪ Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). ▪ Approval of documented evidence by senior management. ▪ Performance of the targeted analysis of risk at least once every 12 months.	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	This requirement is part of the customized approach and must be met for those using the customized approach.
12.3.3	N/A	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: ▪ An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. ▪ Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. ▪ A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	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	The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.
12.3.3	N/A	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: ▪ An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. ▪ Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. ▪ A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5	The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.
12.3.4	N/A	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: ▪ Analysis that the technologies continue to receive security fixes from vendors promptly. ▪ Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. ▪ Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. ▪ Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	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	The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.
12.3.4	N/A	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: ▪ Analysis that the technologies continue to receive security fixes from vendors promptly. ▪ Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. ▪ Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. ▪ Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	Functional	Intersects With	Technical Debt Reviews	SEA-02.3	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	5	The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.3.4	N/A	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: ▪ Analysis that the technologies continue to receive security fixes from vendors promptly. ▪ Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. ▪ Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. ▪ Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.
12.4	N/A	PCI DSS compliance is managed.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
12.4	N/A	PCI DSS compliance is managed.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
12.4	N/A	PCI DSS compliance is managed.	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	
12.4.1	N/A	Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: ▪ Overall accountability for maintaining PCI DSS compliance. ▪ Defining a charter for a PCI DSS compliance program and communication to executive management.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.	5	Executives are responsible and accountable for security of cardholder data.
12.4.1	N/A	Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: ▪ Overall accountability for maintaining PCI DSS compliance. ▪ Defining a charter for a PCI DSS compliance program and communication to executive management.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	Executives are responsible and accountable for security of cardholder data.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	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	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	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	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2	N/A	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: ▪ Daily log reviews. ▪ Configuration reviews for network security controls. ▪ Applying configuration standards to new systems. ▪ Responding to security alerts. ▪ Change-management processes.	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 cybersecurity & data privacy controls.	5	The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.
12.4.2.1	N/A	Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: ▪ Results of the reviews. ▪ Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. ▪ Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.
12.4.2.1	N/A	Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: ▪ Results of the reviews. ▪ Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. ▪ Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.
12.4.2.1	N/A	Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: ▪ Results of the reviews. ▪ Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. ▪ Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.
12.4.2.1	N/A	Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: ▪ Results of the reviews. ▪ Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. ▪ Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	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 cybersecurity & data privacy controls.	5	Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.
12.5	N/A	PCI DSS scope is documented and validated.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
12.5.1	N/A	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Functional	Intersects With	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	All system components in scope for PCI DSS are identified and known.
12.5.1	N/A	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	All system components in scope for PCI DSS are identified and known.
12.5.1	N/A	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all systems, applications and services that collect, receive, process, store, transmit, update and/or share Personal Data (PD).	5	All system components in scope for PCI DSS are identified and known.
12.5.2	N/A	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections from third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	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	PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.5.2	N/A	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections from third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.
12.5.2	N/A	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections from third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.
12.5.2	N/A	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections from third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.
12.5.2	N/A	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections from third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	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	PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.
12.5.2.1	N/A	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries.	5	The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.
12.5.2.1	N/A	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	Functional	Intersects With	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.
12.5.2.1	N/A	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	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	The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.
12.5.2.1	N/A	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.
12.5.3	N/A	Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	PCI DSS scope is confirmed after significant organizational change.
12.6	N/A	Security awareness education is an ongoing activity.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
12.6	N/A	Security awareness education is an ongoing activity.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	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 (optional)	Notes (optional)
12.6	N/A	Security awareness education is an ongoing activity.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
12.6	N/A	Security awareness education is an ongoing activity.	Functional	Intersects With	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-system training.	5	
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.1	N/A	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	Functional	Intersects With	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-system 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.
12.6.2	N/A	The security awareness program is: ▪ Reviewed at least once every 12 months, and ▪ Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	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	The content of security awareness material is reviewed and updated periodically.
12.6.2	N/A	The security awareness program is: ▪ Reviewed at least once every 12 months, and ▪ Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	The content of security awareness material is reviewed and updated periodically.
12.6.3	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	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	Personnel remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	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 remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity & data privacy policies and provide acknowledgement.	5	Personnel remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Personnel remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	Personnel remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-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 remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Intersects With	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-system training.	5	Personnel remain 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	N/A	Personnel receive security awareness training as follows: ▪ Upon hire and at least once every 12 months. ▪ Multiple methods of communication are used. ▪ Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.
12.6.3.1	N/A	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ▪ Phishing and related attacks. ▪ Social engineering.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	N/A	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ▪ Phishing and related attacks. ▪ Social engineering.	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	N/A	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ▪ Phishing and related attacks. ▪ Social engineering.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	N/A	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ▪ Phishing and related attacks. ▪ Social engineering.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.
12.6.3.1	N/A	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: ▪ Phishing and related attacks. ▪ Social engineering.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy 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.
12.6.3.2	N/A	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-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 responsibility for the security and operation of end- user technologies and are able to access assistance and guidance when required.
12.6.3.2	N/A	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	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 responsibility for the security and operation of end- user technologies and are able to access assistance and guidance when required.
12.6.3.2	N/A	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy 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 responsibility for the security and operation of end- user technologies and are able to access assistance and guidance when required.
12.7	N/A	Personnel are screened to reduce risks from insider threats.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
12.7	N/A	Personnel are screened to reduce risks from insider threats.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
12.7	N/A	Personnel are screened to reduce risks from insider threats.	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.	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 (optional)	Notes (optional)
12.7	N/A	Personnel are screened to reduce risks from insider threats.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
12.7	N/A	Personnel are screened to reduce risks from insider threats.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
12.7.1	N/A	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	The risk related to allowing new members of staff access to the CDE is understood and managed.
12.7.1	N/A	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	The risk related to allowing new members of staff access to the CDE is understood and managed.
12.7.1	N/A	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.	5	The risk related to allowing new members of staff access to the CDE is understood and managed.
12.7.1	N/A	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	The risk related to allowing new members of staff access to the CDE is understood and managed.
12.7.1	N/A	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	The risk related to allowing new members of staff access to the CDE is understood and managed.
12.8	N/A	Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
12.8	N/A	Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
12.8	N/A	Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	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 systems, applications, services and data.	5	
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	Records are maintained of TPSPs and the services provided.
12.8.1	N/A	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	Records are maintained of TPSPs and the services provided.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.2	N/A	Written agreements with TPSPs are maintained as follows: ▪ Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. ▪ Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.
12.8.3	N/A	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.
12.8.4	N/A	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	The PCI DSS compliance status of TPSPs is verified periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.
12.8.5	N/A	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy 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.
12.9	N/A	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
12.9	N/A	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
12.9	N/A	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
12.9	N/A	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
12.9.1	N/A	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	TPSPs formally acknowledge their security responsibilities to their customers.
12.9.1	N/A	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	TPSPs formally acknowledge their security responsibilities to their customers.
12.9.1	N/A	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer'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 systems and data.	5	TPSPs formally acknowledge their security responsibilities to their customers.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.9.1	N/A	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	TPSPs formally acknowledge their security responsibilities to their customers.
12.9.1	N/A	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	TPSPs formally acknowledge their security responsibilities to their customers.
12.9.2	N/A	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: ▪ PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). ▪ Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.
12.9.2	N/A	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: ▪ PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). ▪ Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.
12.9.2	N/A	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: ▪ PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). ▪ Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.
12.9.2	N/A	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: ▪ PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). ▪ Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.
12.10	N/A	Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
12.10	N/A	Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
12.10	N/A	Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
12.10	N/A	Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	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	
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	A comprehensive incident response plan that meets card brand expectations is maintained.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.10.1	N/A	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: ▪ Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. ▪ Incident response procedures with specific containment and mitigation activities for different types of incidents. ▪ Business recovery and continuity procedures. ▪ Data backup processes. ▪ Analysis of legal requirements for reporting compromises. ▪ Coverage and responses of all critical system components. ▪ Reference or inclusion of incident response procedures from the payment brands.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	A comprehensive incident response plan that meets card brand expectations is maintained.
12.10.2	N/A	At least once every 12 months, the security incident response plan is: ▪ Reviewed and the content is updated as needed. ▪ Tested, including all elements listed in Requirement 12.10.1.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	The incident response plan is kept current and tested periodically.
12.10.2	N/A	At least once every 12 months, the security incident response plan is: ▪ Reviewed and the content is updated as needed. ▪ Tested, including all elements listed in Requirement 12.10.1.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	The incident response plan is kept current and tested periodically.
12.10.3	N/A	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 & data privacy incident response operations.	5	Incidents are responded to immediately where appropriate.
12.10.4	N/A	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.
12.10.4.1	N/A	The frequency of periodic training for incident response personnel 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	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	Incident response personnel are trained at a frequency that addresses the entity's risk.
12.10.5	N/A	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: ▪ Intrusion-detection and intrusion-prevention systems. ▪ Network security controls. ▪ Change-detection mechanisms for critical files. ▪ The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Detection of unauthorized wireless access points.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.
12.10.5	N/A	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: ▪ Intrusion-detection and intrusion-prevention systems. ▪ Network security controls. ▪ Change-detection mechanisms for critical files. ▪ The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Detection of unauthorized wireless access points.	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	Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.
12.10.5	N/A	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: ▪ Intrusion-detection and intrusion-prevention systems. ▪ Network security controls. ▪ Change-detection mechanisms for critical files. ▪ The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Detection of unauthorized wireless access points.	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	Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.
12.10.5	N/A	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: ▪ Intrusion-detection and intrusion-prevention systems. ▪ Network security controls. ▪ Change-detection mechanisms for critical files. ▪ The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Detection of unauthorized wireless access points.	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	Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.
12.10.6	N/A	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.
12.10.6	N/A	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.
12.10.7	N/A	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: ▪ Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. ▪ Identifying whether sensitive authentication data is stored with PAN. ▪ Determining where the account data came from and how it ended up where it was not expected. ▪ Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	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	Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.
12.10.7	N/A	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: ▪ Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. ▪ Identifying whether sensitive authentication data is stored with PAN. ▪ Determining where the account data came from and how it ended up where it was not expected. ▪ Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	Functional	Intersects With	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.	5	Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.
12.10.7	N/A	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: ▪ Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. ▪ Identifying whether sensitive authentication data is stored with PAN. ▪ Determining where the account data came from and how it ended up where it was not expected. ▪ Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	Functional	Intersects With	Post-Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	5	Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.
A1.1	N/A	Multi-tenant service providers protect and separate all customer environments and data.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
A1.1.1	N/A	Logical separation is implemented as follows: ▪ The provider cannot access its customers' environments without authorization. ▪ Customers cannot access the provider's environment without authorization.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	Customers cannot access the provider's environment. The provider cannot access its customers' environments without authorization.
A1.1.2	N/A	Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	Customers cannot access other customers' environments.
A1.1.3	N/A	Controls are implemented such that each customer can only access resources allocated to them.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	Customers cannot impact resources allocated to other customers.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A1.1.4	N/A	The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	Segmentation of customer environments from other environments is periodically validated to be effective.
A1.1.4	N/A	The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	Segmentation of customer environments from other environments is periodically validated to be effective.
A1.1.4	N/A	The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	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	Segmentation of customer environments from other environments is periodically validated to be effective.
A1.2	N/A	Multi-tenant service providers facilitate logging and incident response for all customers.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-06.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5	
A1.2	N/A	Multi-tenant service providers facilitate logging and incident response for all customers.	Functional	Intersects With	Multi-Tenant Forensics Capabilities	CLD-06.3	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt forensic investigations in the event of a suspected or confirmed security incident.	5	
A1.2	N/A	Multi-tenant service providers facilitate logging and incident response for all customers.	Functional	Intersects With	Multi-Tenant Incident Response Capabilities	CLD-06.4	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers.	5	
A1.2.1	N/A	Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: ▪ Logs are enabled for common third-party applications. ▪ Logs are active by default. ▪ Logs are available for review only by the owning customer. ▪ Log locations are clearly communicated to the owning customer. ▪ Log data and availability is consistent with PCI DSS Requirement 10.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-06.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5	Log capability is available to all customers without affecting the confidentiality of other customers.
A1.2.2	N/A	Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.	Functional	Intersects With	Multi-Tenant Forensics Capabilities	CLD-06.3	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt forensic investigations in the event of a suspected or confirmed security incident.	5	Forensic investigation is readily available to all customers in the event of a suspected or confirmed security incident.
A1.2.3	N/A	Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: ▪ Customers can securely report security incidents and vulnerabilities to the provider. ▪ The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	Functional	Intersects With	Multi-Tenant Incident Response Capabilities	CLD-06.4	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers.	5	Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.
A1.2.3	N/A	Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: ▪ Customers can securely report security incidents and vulnerabilities to the provider. ▪ The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.
A1.2.3	N/A	Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: ▪ Customers can securely report security incidents and vulnerabilities to the provider. ▪ The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	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	Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.
A1.2.3	N/A	Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: ▪ Customers can securely report security incidents and vulnerabilities to the provider. ▪ The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.
A2.1	N/A	POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
A2.1	N/A	POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.	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	
A2.1.1	N/A	Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	This requirement is not eligible for the customized approach.
A2.1.1	N/A	Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	Functional	Intersects With	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5	This requirement is not eligible for the customized approach.
A2.1.2	N/A	Additional requirement for service providers only: All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: ▪ Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. ▪ Risk-assessment results and risk-reduction controls in place. ▪ Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. ▪ Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments. ▪ Overview of migration project plan to replace SSL/early TLS at a future date.	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.
A2.1.2	N/A	Additional requirement for service providers only: All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: ▪ Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. ▪ Risk-assessment results and risk-reduction controls in place. ▪ Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. ▪ Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments. ▪ Overview of migration project plan to replace SSL/early TLS at a future date.	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.
A2.1.3	N/A	Additional requirement for service providers only: All service providers provide a secure service offering.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	This requirement is not eligible for the customized approach.
A3.1	N/A	A PCI DSS compliance program is implemented.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
A3.1.1	N/A	Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes: ▪ Overall accountability for maintaining PCI DSS compliance. ▪ Defining a charter for a PCI DSS compliance program. ▪ Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months. PCI DSS Reference: Requirement 12	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	This requirement is not eligible for the customized approach.
A3.1.1	N/A	Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes: ▪ Overall accountability for maintaining PCI DSS compliance. ▪ Defining a charter for a PCI DSS compliance program. ▪ Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months. PCI DSS Reference: Requirement 12	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A3.1.2	N/A	A formal PCI DSS compliance program is in place that includes: ▪ Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities. ▪ Annual PCI DSS assessment processes. ▪ Processes for the continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). ▪ A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirements 1-12	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	This requirement is not eligible for the customized approach.
A3.1.3	N/A	PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including: ▪ Managing PCI DSS business-as-usual activities. ▪ Managing annual PCI DSS assessments. ▪ Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). ▪ Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirement 12	Functional	Intersects With	Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	This requirement is not eligible for the customized approach.
A3.1.3	N/A	PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including: ▪ Managing PCI DSS business-as-usual activities. ▪ Managing annual PCI DSS assessments. ▪ Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). ▪ Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirement 12	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	This requirement is not eligible for the customized approach.
A3.1.4	N/A	Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). PCI DSS Reference: Requirement 12	Functional	Intersects With	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	This requirement is not eligible for the customized approach.
A3.1.4	N/A	Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). PCI DSS Reference: Requirement 12	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	This requirement is not eligible for the customized approach.
A3.2	N/A	PCI DSS scope is documented and validated.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
A3.2.1	N/A	PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in- scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections to third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	This requirement is not eligible for the customized approach.
A3.2.1	N/A	PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in- scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections to third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A3.2.1	N/A	PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in- scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections to third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12.	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	This requirement is not eligible for the customized approach.
A3.2.1	N/A	PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in- scope environment. At a minimum, the scoping validation includes: ▪ Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). ▪ Updating all data-flow diagrams per Requirement 1.2.4. ▪ Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. ▪ For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. ▪ Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. ▪ Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. ▪ Identifying all connections to third-party entities with access to the CDE. ▪ Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	This requirement is not eligible for the customized approach.
A3.2.2	N/A	PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: ▪ Performing a formal PCI DSS impact assessment. ▪ Identifying applicable PCI DSS requirements to the system or network. ▪ Updating PCI DSS scope as appropriate. ▪ Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). PCI DSS Reference: Scope of PCI DSS Requirements; Requirements 1-12	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	This requirement is not eligible for the customized approach.
A3.2.2	N/A	PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: ▪ Performing a formal PCI DSS impact assessment. ▪ Identifying applicable PCI DSS requirements to the system or network. ▪ Updating PCI DSS scope as appropriate. ▪ Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). PCI DSS Reference: Scope of PCI DSS Requirements; Requirements 1-12	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	This requirement is not eligible for the customized approach.
A3.2.2	N/A	PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: ▪ Performing a formal PCI DSS impact assessment. ▪ Identifying applicable PCI DSS requirements to the system or network. ▪ Updating PCI DSS scope as appropriate. ▪ Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). PCI DSS Reference: Scope of PCI DSS Requirements; Requirements 1-12	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	This requirement is not eligible for the customized approach.
A3.2.2.1	N/A	Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. PCI DSS Reference: Scope of PCI DSS Requirements; Requirement 1-12	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	This requirement is not eligible for the customized approach.
A3.2.2.1	N/A	Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. PCI DSS Reference: Scope of PCI DSS Requirements; Requirement 1-12	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5	This requirement is not eligible for the customized approach.
A3.2.3	N/A	Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. PCI DSS Reference: Requirement 12	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	This requirement is not eligible for the customized approach.
A3.2.3	N/A	Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. PCI DSS Reference: Requirement 12	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	This requirement is not eligible for the customized approach.
A3.2.3	N/A	Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. PCI DSS Reference: Requirement 12	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	This requirement is not eligible for the customized approach.
A3.2.4	N/A	If segmentation is used, PCI DSS scope is confirmed as follows: ▪ Per the entity's methodology defined at Requirement 11.4.1. ▪ Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. ▪ The penetration testing covers all segmentation controls/methods in use. ▪ The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out- of-scope systems. PCI DSS Reference: Requirement 11	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A3.2.4	N/A	If segmentation is used, PCI DSS scope is confirmed as follows: ▪ Per the entity's methodology defined at Requirement 11.4.1. ▪ Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. ▪ The penetration testing covers all segmentation controls/methods in use. ▪ The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out- of-scope systems. PCI DSS Reference: Requirement 11	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	This requirement is not eligible for the customized approach.
A3.2.4	N/A	If segmentation is used, PCI DSS scope is confirmed as follows: ▪ Per the entity's methodology defined at Requirement 11.4.1. ▪ Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. ▪ The penetration testing covers all segmentation controls/methods in use. ▪ The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out- of-scope systems. PCI DSS Reference: Requirement 11	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	This requirement is not eligible for the customized approach.
A3.2.5	N/A	A data-discovery methodology is implemented that: ▪ Confirms PCI DSS scope. ▪ Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. ▪ Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	This requirement is not eligible for the customized approach
A3.2.5	N/A	A data-discovery methodology is implemented that: ▪ Confirms PCI DSS scope. ▪ Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. ▪ Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries.	5	This requirement is not eligible for the customized approach
A3.2.5	N/A	A data-discovery methodology is implemented that: ▪ Confirms PCI DSS scope. ▪ Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. ▪ Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	This requirement is not eligible for the customized approach
A3.2.5	N/A	A data-discovery methodology is implemented that: ▪ Confirms PCI DSS scope. ▪ Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. ▪ Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	5	This requirement is not eligible for the customized approach
A3.2.5	N/A	A data-discovery methodology is implemented that: ▪ Confirms PCI DSS scope. ▪ Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. ▪ Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	This requirement is not eligible for the customized approach
A3.2.5.1	N/A	Data discovery methods are confirmed as follows: ▪ Effectiveness of methods is tested. ▪ Methods are able to discover cleartext PAN on all types of system components and file formats in use. ▪ The effectiveness of data-discovery methods is confirmed at least once every 12 months. PCI DSS Reference: Scope of PCI DSS Requirements	Functional	Intersects With	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	5	This requirement is not eligible for the customized approach.
A3.2.5.2	N/A	Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include: ▪ Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. ▪ Determining how the data ended up outside the CDE. ▪ Remediating data leaks or process gaps that resulted in the data being outside the CDE. ▪ Identifying the source of the data. ▪ Identifying whether any track data is stored with the PANs.	Functional	Intersects With	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.	5	This requirement is not eligible for the customized approach.
A3.2.5.2	N/A	Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include: ▪ Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. ▪ Determining how the data ended up outside the CDE. ▪ Remediating data leaks or process gaps that resulted in the data being outside the CDE. ▪ Identifying the source of the data. ▪ Identifying whether any track data is stored with the PANs.	Functional	Intersects With	Post-Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	5	This requirement is not eligible for the customized approach.
A3.2.6	N/A	Mechanisms are implemented for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including mechanisms that are: ▪ Actively running. ▪ Configured to detect and prevent cleartext PAN leaving the CDE via an unauthorized channel, method, or process. ▪ Generating audit logs and alerts upon detection of cleartext PAN leaving the CDE via an unauthorized channel, method, or process. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	This requirement is not eligible for the customized approach.
A3.2.6.1	N/A	Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: ▪ Procedures for the prompt investigation of alerts by responsible personnel. ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Mechanisms exist to automatically implement pre-determined corrective actions in response to detected events that have security incident implications.	5	This requirement is not eligible for the customized approach.
A3.2.6.1	N/A	Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: ▪ Procedures for the prompt investigation of alerts by responsible personnel. ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	This requirement is not eligible for the customized approach.
A3.2.6.1	N/A	Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: ▪ Procedures for the prompt investigation of alerts by responsible personnel. ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A3.2.6.1	N/A	Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: ▪ Procedures for the prompt investigation of alerts by responsible personnel. ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12	Functional	Intersects With	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5	This requirement is not eligible for the customized approach.
A3.2.6.1	N/A	Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: ▪ Procedures for the prompt investigation of alerts by responsible personnel. ▪ Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12	Functional	Intersects With	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	5	This requirement is not eligible for the customized approach.
A3.3	N/A	PCI DSS is incorporated into business-as-usual (BAU) activities.	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
A3.3.1	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: ▪ Network security controls ▪ IDS/IPS ▪ FIM ▪ Anti-malware solutions ▪ Physical access controls ▪ Logical access controls ▪ Audit logging mechanisms ▪ Segmentation controls (if used) ▪ Automated audit log review mechanisms. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Automated code review tools (if used). This bullet is a best practice until its effective date; refer to Applicability Notes below for details. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	This requirement is not eligible for the customized approach.
A3.3.1	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: ▪ Network security controls ▪ IDS/IPS ▪ FIM ▪ Anti-malware solutions ▪ Physical access controls ▪ Logical access controls ▪ Audit logging mechanisms ▪ Segmentation controls (if used) ▪ Automated audit log review mechanisms. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Automated code review tools (if used). This bullet is a best practice until its effective date; refer to Applicability Notes below for details. PCI DSS Reference: Requirements 1-12	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	This requirement is not eligible for the customized approach.
A3.3.1	N/A	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: ▪ Network security controls ▪ IDS/IPS ▪ FIM ▪ Anti-malware solutions ▪ Physical access controls ▪ Logical access controls ▪ Audit logging mechanisms ▪ Segmentation controls (if used) ▪ Automated audit log review mechanisms. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ▪ Automated code review tools (if used). This bullet is a best practice until its effective date; refer to Applicability Notes below for details. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	5	
A3.3.1.2	N/A	Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	This requirement is not eligible for the customized approach.
A3.3.1.2	N/A	Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	This requirement is not eligible for the customized approach.
A3.3.1.2	N/A	Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	This requirement is not eligible for the customized approach.

FDE #	FDE Name	Focal Document Element (FDE) Description▪	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A3.3.1.2	N/A	Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	This requirement is not eligible for the customized approach.
A3.3.1.2	N/A	Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: ▪ Restoring security functions. ▪ Identifying and documenting the duration (date and time from start to end) of the security failure. ▪ Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. ▪ Identifying and addressing any security issues that arose during the failure. ▪ Determining whether further actions are required as a result of the security failure. ▪ Implementing controls to prevent the cause of failure from reoccurring. ▪ Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12	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.
A3.3.2	N/A	Hardware and software technologies are reviewed at least once every 12 months to confirm whether they continue to meet the organization's PCI DSS requirements. PCI DSS Reference: Requirements 2, 6, 12.	Functional	Intersects With	Technical Debt Reviews	SEA-02.3	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	5	This requirement is not eligible for the customized approach.
A3.3.3	N/A	Reviews are performed at least once every three months to verify BAU activities are being followed. Reviews are performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include: ▪ Confirmation that all BAU activities, including A3.2.2, A3.2.6, and A3.3.1, are being performed. ▪ Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, ruleset reviews for network security controls, configuration standards for new systems). ▪ Documenting how the reviews were completed, including how all BAU activities were verified as being in place. ▪ Collection of documented evidence as required for the annual PCI DSS assessment. ▪ Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program, as identified in A3.1.3. ▪ Retention of records and documentation for at least 12 months, covering all BAU activities. PCI DSS Reference: Requirements 1-12	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	5	This requirement is not eligible for the customized approach.
A3.4	N/A	Logical access to the cardholder data environment is controlled and managed.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
A3.4.1	N/A	User accounts and access privileges to in- scope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized. PCI DSS Reference: Requirement 7	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	This requirement is not eligible for the customized approach.
A3.5	N/A	Suspicious events are identified and responded to.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
A3.5	N/A	Suspicious events are identified and responded to.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
A3.5	N/A	Suspicious events are identified and responded to.	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Mechanisms exist to automatically implement pre-determined corrective actions in response to detected events that have security incident implications.	5	
A3.5.1	N/A	A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: ▪ Identification of anomalies or suspicious activity as it occurs. ▪ Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. ▪ Response to alerts in accordance with documented response procedures. PCI DSS Reference: Requirements 10, 12	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	This requirement is not eligible for the customized approach.