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

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

Focal Document: SWIFT Customer Security Controls Framework 2025
Focal Document URL: https://www2.swift.com/knowledgecentre/publications/cscf_dd/70.0
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-swift-cscf-2025.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Restrict Internet Access and Protect Critical Systems from General IT Environment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	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	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	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	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	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	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	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	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	3	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	8	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	5	
1.1	Swift Environment Protection	A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
1.2	Operating System Privileged Account Control	Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
1.2	Operating System Privileged Account Control	Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
1.2	Operating System Privileged Account Control	Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.	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.	8	
1.2	Operating System Privileged Account Control	Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	8	
1.2	Operating System Privileged Account Control	Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
1.3	Virtualisation or Cloud Platform Protection	Secure the virtualisation or cloud platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
1.3	Virtualisation or Cloud Platform Protection	Secure the virtualisation or cloud platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
1.3	Virtualisation or Cloud Platform Protection	Secure the virtualisation or cloud platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
1.3	Virtualisation or Cloud Platform Protection	Secure the virtualisation or cloud platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.	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 security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
1.3	Virtualisation or Cloud Platform Protection	Secure the virtualisation or cloud platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	8	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	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	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	5	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive/regulated data enclaves (secure zones).	8	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	8	
1.4	Restriction of Internet Access	All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Jump Server	AST-27	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	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.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	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.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	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).	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8	
1.5	Customer Environment Protection	A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
2	Reduce Attack Surface and Vulnerabilities	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	8	
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	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	
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	Functional	Intersects With	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	3	
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	8	
2.1	Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-tocomponent or system-to-system data flows.	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	5	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	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.	8	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Deferred Patching Decisions	VPM-04.3	Mechanisms exist to facilitate the deferral of software and/or firmware patches when the disadvantages of applying the patch outweighs the benefits.	5	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	8	
2.2	Security Updates	All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.	Functional	Intersects With	Software Patch Integrity	VPM-05.8	Mechanisms exist to ensure software and/or firmware patches are:(1) Obtained from trusted sources; and(2) Checked for integrity.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	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.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	3	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	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.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	8	
2.3	System Hardening	Security hardening is conducted and maintained on all in-scope 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.	8	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	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	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	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	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	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	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	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	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	
2.4	Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms (at system, transport, message, or data level) are implemented to protect data exchanged between user's Swift infrastructure components and the back-office first hops they connect to.	Functional	Intersects With	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	5	
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	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.	3	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	No explanation for the numbering difference for "2.5A"
2.5A	External Transmission Data Protection	Sensitive Swift-related data that leaves the secure zone as a result of operating system or application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit to the first storage location.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	8	No explanation for the numbering difference for "2.5A"
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Jump Server	AST-27	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.	5	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	
2.6	Operator Session Confidentiality and Integrity	The confidentiality and integrity of interactive operator sessions that connect to service provider Swift-related applications or into the user's secure zone are safeguarded.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	8	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	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.	8	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	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	
2.7	Vulnerability Scanning	Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities at OS and application level using an up-to-date, reputable scanning tool and results, reported by the tool, are considered for appropriate resolving actions.	Functional	Intersects With	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	5	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	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.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:(1) Contractual obligations for the External Service Provider (ESP);(2) Business practices;(3) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	3	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	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.	8	
2.8	Outsourced Critical Activity Protection	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.	8	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	5	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	Functional	Intersects With	Transfer Activity Limits	DCH-25.1	Mechanisms exist to establish organization-defined "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) fraudulent actions.	5	
2.9	Transaction Business Controls	Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business.	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	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	8	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.	8	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	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.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope components.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
2.10	Application Hardening	All messaging interfaces and communication interfaces products within the Swift secure zone are Swiftcompatible. Application security hardening is conducted and maintained on all in-scope 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.	8	
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	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	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	No explanation for the numbering difference for "2.11A"
2.11A	RMA Business Controls	Implement RMA controls to restrict transaction activity to effective business counterparties.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	No explanation for the numbering difference for "2.11A"
3	Physically Secure the Environment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	8	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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).	8	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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).	8	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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.	8	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	8	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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	
3.1	Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.	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	
4	Prevent Compromise of Credentials	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
4.1	Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
4.1	Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
4.1	Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
4.1	Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.	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.	8	
4.2	Multi-Factor Authentication	Multi-factor authentication is used for interactive user access to Swift-related components or applications and operating system accounts.	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	10	
5	Manage Identities and Separate Privileges	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	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	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	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	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	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	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
5.1	Logical Access Control	Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties.	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.	8	
5.2	Token Management	Connected and disconnected hardware authentication or personal and software tokens are managed appropriately during their assignment, distribution, revocation, use, and storage.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
5.2	Token Management	Connected and disconnected hardware authentication or personal and software tokens are managed appropriately during their assignment, distribution, revocation, use, and storage.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
5.2	Token Management	Connected and disconnected hardware authentication or personal and software tokens are managed appropriately during their assignment, distribution, revocation, use, and storage.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
5.2	Token Management	Connected and disconnected hardware authentication or personal and software tokens are managed appropriately during their assignment, distribution, revocation, use, and storage.	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.	8	
5.3A	Staff Screening Process	Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	No explanation for the numbering difference for "5.3A"
5.3A	Staff Screening Process	Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter.	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive/regulated data is cleared and regularly trained to handle the information in question.	8	No explanation for the numbering difference for "5.3A"
5.3A	Staff Screening Process	Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	No explanation for the numbering difference for "5.3A"
5.3A	Staff Screening Process	Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter.	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.	8	No explanation for the numbering difference for "5.3A"
5.3A	Staff Screening Process	Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter.	Functional	Intersects With	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	8	No explanation for the numbering difference for "5.3A"
5.4	Password Repository Protection	Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-toknow basis.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
5.4	Password Repository Protection	Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-toknow basis.	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.	8	
5.4	Password Repository Protection	Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-toknow basis.	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.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.4	Password Repository Protection	Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-toknow basis.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	8	
6	Detect Anomalous Activity to Systems or Transaction Records	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	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	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	8	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
6.1	Malware Protection	Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. An Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR), offering similar control on the infrastructure can be considered as a valid implementation.	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	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	8	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	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	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	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.	8	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	8	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
6.2	Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time.	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	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	8	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	Functional	Intersects With	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	8	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	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.	8	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
6.3	Database Integrity	A database integrity check is performed at regular intervals on databases that record transactions and results are considered for appropriate resolving actions.	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	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	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	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	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.	8	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	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	
6.4	Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs.	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	
6.5A	Intrusion Detection	Intrusion detection is implemented to detect unauthorised network access and anomalous activity.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	No explanation for the numbering difference for "6.5A"
6.5A	Intrusion Detection	Intrusion detection is implemented to detect unauthorised network access and anomalous activity.	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.	8	No explanation for the numbering difference for "6.5A"
6.5A	Intrusion Detection	Intrusion detection is implemented to detect unauthorised network access and anomalous activity.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	8	No explanation for the numbering difference for "6.5A"
6.5A	Intrusion Detection	Intrusion detection is implemented to detect unauthorised network access and anomalous activity.	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.	8	No explanation for the numbering difference for "6.5A"
7	Plan for Incident Response and Information Sharing	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1	Cyber Incident Response Planning	The user has a defined and tested cyber incident response plan.	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 and data protection-related incidents.	10	
7.1	Cyber Incident Response Planning	The user has a defined and tested cyber incident response plan.	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.	8	
7.1	Cyber Incident Response Planning	The user has a defined and tested cyber incident response plan.	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.	3	
7.1	Cyber Incident Response Planning	The user has a defined and tested cyber incident response plan.	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.	8	
7.1	Cyber Incident Response Planning	The user has a defined and tested cyber incident response plan.	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.	8	
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to:(1) Organizational policies, standards and procedures;(2) Assigned roles and responsibilities;(3) Relevant threats and risks; and(4) Technological developments.	5	
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	8	
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	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.	8	
7.2	Security Training and Awareness	Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion).	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	8	
7.3A	Penetration Testing	Application, system, and network penetration testing is regularly conducted towards the secure zone, the Swiftrelated components and the dedicated operator PCs or, when used, the jump servers.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	No explanation for the numbering difference for "7.3A"
7.3A	Penetration Testing	Application, system, and network penetration testing is regularly conducted towards the secure zone, the Swiftrelated components and the dedicated operator PCs or, when used, the jump servers.	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	8	No explanation for the numbering difference for "7.3A"
7.3A	Penetration Testing	Application, system, and network penetration testing is regularly conducted towards the secure zone, the Swiftrelated components and the dedicated operator PCs or, when used, the jump servers.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	No explanation for the numbering difference for "7.3A"
7.4A	Scenario-based Risk Assessment	Scenario-based risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organisation's security programme.	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	No explanation for the numbering difference for "7.4A"