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: **Committee of Sponsoring Organizations (COSO) (2013)**
Focal Document URL: https://www.coso.org/_files/ugd/3059fc_c98a93b420a34d28a4c79f57db0d2c93.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-coso-2013.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	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
1	N/A	Demonstrates commitment to integrity and ethical values	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
2	N/A	Exercises oversight responsibility	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	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
2	N/A	Exercises oversight responsibility	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
3	N/A	Establishes structure, authority, and responsibility	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3	N/A	Establishes structure, authority, and responsibility	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3	N/A	Establishes structure, authority, and responsibility	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3	N/A	Establishes structure, authority, and responsibility	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3	N/A	Establishes structure, authority, and responsibility	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
3	N/A	Establishes structure, authority, and responsibility	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.	5	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
4	N/A	Demonstrates commitment to competence	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.	5	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
4	N/A	Demonstrates commitment to competence	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	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5	
4	N/A	Demonstrates commitment to competence	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
5	N/A	Enforces accountability	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
5	N/A	Enforces accountability	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
5	N/A	Enforces accountability	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
5	N/A	Enforces accountability	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
6	N/A	Specifies suitable objectives	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
6	N/A	Specifies suitable objectives	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
6	N/A	Specifies suitable objectives	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
6	N/A	Specifies suitable objectives	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6	N/A	Specifies suitable objectives	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.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
7	N/A	Identifies and analyzes risk	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	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Incidents;	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
7	N/A	Identifies and analyzes risk	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
8	N/A	Assesses fraud risk	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	
8	N/A	Assesses fraud risk	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
8	N/A	Assesses fraud risk	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	
8	N/A	Assesses fraud risk	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
8	N/A	Assesses fraud risk	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
9	N/A	Identifies and analyzes significant change	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.	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
9	N/A	Identifies and analyzes significant change	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
9	N/A	Identifies and analyzes significant change	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.	5	
10	N/A	Selects and develops control activities	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
10	N/A	Selects and develops control activities	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
10	N/A	Selects and develops control activities	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.	5	
10	N/A	Selects and develops control activities	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).	5	
10	N/A	Selects and develops control activities	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
10	N/A	Selects and develops control activities	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.	5	
10	N/A	Selects and develops control activities	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
10	N/A	Selects and develops control activities	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11	N/A	Selects and develops general controls over technology	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).	5	
11	N/A	Selects and develops general controls over technology	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.	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
11	N/A	Selects and develops general controls over technology	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).	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
11	N/A	Selects and develops general controls over technology	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
12	N/A	Deploys through policies and procedures	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
12	N/A	Deploys through policies and procedures	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
12	N/A	Deploys through policies and procedures	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
12	N/A	Deploys through policies and procedures	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
12	N/A	Deploys through policies and procedures	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
13	N/A	Uses relevant information	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	
13	N/A	Uses relevant information	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
13	N/A	Uses relevant information	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
13	N/A	Uses relevant information	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
13	N/A	Uses relevant information	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	
13	N/A	Uses relevant information	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
13	N/A	Uses relevant information	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
14	N/A	Communicates internally	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
14	N/A	Communicates internally	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
14	N/A	Communicates internally	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
14	N/A	Communicates internally	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
14	N/A	Communicates internally	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
14	N/A	Communicates internally	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
14	N/A	Communicates internally	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
14	N/A	Communicates internally	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).	5	
14	N/A	Communicates internally	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).	5	
14	N/A	Communicates internally	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
14	N/A	Communicates internally	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
14	N/A	Communicates internally	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
15	N/A	Communicates externally	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
15	N/A	Communicates externally	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
15	N/A	Communicates externally	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
15	N/A	Communicates externally	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
15	N/A	Communicates externally	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
15	N/A	Communicates externally	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	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
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
16	N/A	Conducts ongoing and/or separate evaluations	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).	5	
16	N/A	Conducts ongoing and/or separate evaluations	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.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
16	N/A	Conducts ongoing and/or separate evaluations	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies);	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
17	N/A	Evaluates and communicates deficiencies	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	