Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.4**
Focal Document: **Canada OSFI-B13**
Focal Document Source: **https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management**
STRM URL: **https://securecontrolsframework.com/content/strm/scf-strm-canada-osfi-b13.pdf**

Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

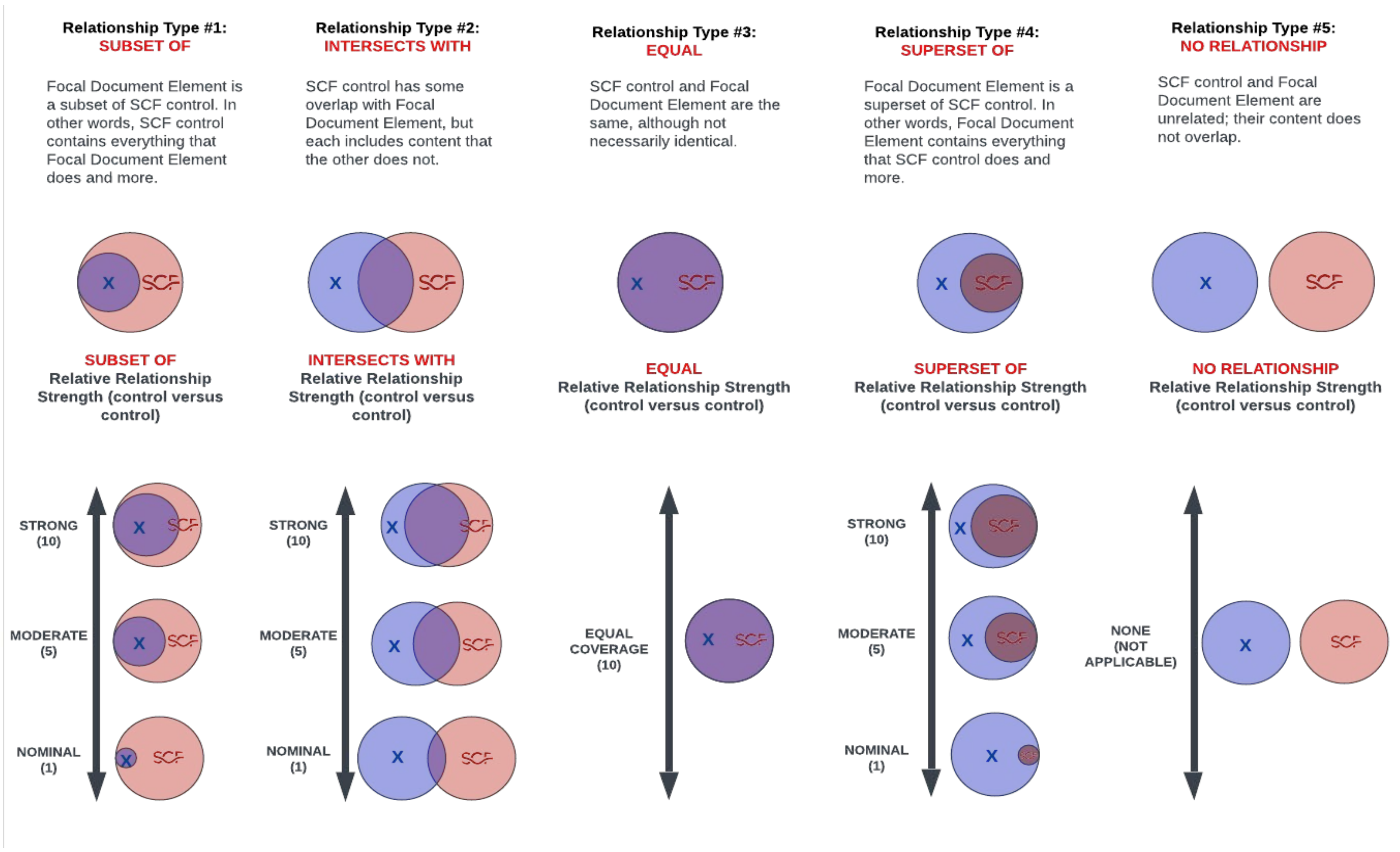
1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**

SCF Reference Document

Law, Regulation or Framework Focal Document



Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.

SUBSET OF Relative Relationship Strength (control versus control)

INTERSECTS WITH Relative Relationship Strength (control versus control)

EQUAL Relative Relationship Strength (control versus control)

SUPERSET OF Relative Relationship Strength (control versus control)

NO RELATIONSHIP Relative Relationship Strength (control versus control)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A	Purpose and scope	This Guideline establishes OSFI's expectations related to technology and cyber risk management. It is applicable to all federally regulated financial institutions (FRFIs), including foreign bank branches and foreign insurance company branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada.Footnote1 Expectations for branches are set out in Guideline E-4 on Foreign Entities Operating in Canada on a Branch Basis. These expectations aim to support FRFIs in developing greater resilience to technology and cyber risks.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	Guidelines - not requirements.
A.1	Definitions	"Technology risk", which includes "cyber risk", refers to the risk arising from the inadequacy, disruption, destruction, failure, damage from unauthorised access, modifications, or malicious use of information technology assets, people or processes that enable and support business needs, and can result in financial loss and/or reputational damage. A "Technology asset" is something tangible (e.g., hardware, infrastructure) or intangible (e.g., software, data, information) that needs protection and supports the provision of technology services. "Technology" is broadly used in this Guideline to include "information technology" (IT), and "cyber" is broadly used to include "information security."	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
A.2	Structure	This Guideline is organized into three domains. Each sets out key components of sound technology and cyber risk management. 1. Governance and risk management – Sets OSFI's expectations for the formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. 2. Technology operations and resilience – Sets OSFI's expectations for management and oversight of risks related to the design, implementation, management and recovery of technology assets and services. 3. Cyber security – Sets OSFI's expectations for management and oversight of cyber risk.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	Guidelines - not requirements.
A.3	Outcomes	Each domain has a desired outcome for FRFIs to achieve through managing risks that contribute to developing FRFIs' resilience to technology and cyber risks.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	Guidelines - not requirements.

A.4	Related guidance and information	Technology and cyber risks are dynamic and intersect with other risk areas. FRFIs should read this Guideline in conjunction with other OSFI guidance, tools and supervisory communications, as well as guidance issued by other authorities applicable to the FRFI's operating environment; in particular:
		OSFI Corporate Governance Guideline;
		OSFI Guideline E-21 (Operational Risk Management);
		OSFI Guideline B-10 (Outsourcing);
		OSFI Cyber Security Self-Assessment Tool;
		OSFI Technology and Cyber Security Incident Reporting Advisory;
		Alerts, advisories and other communications issued by the Canadian Centre for Cyber Security; and
		Recognized frameworks and standards for technology operations and information security.
			Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	Guidelines - not requirements.

1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			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 cybersecurity & data protection program.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			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 data and technology-related risks.	5	
			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 data and technology-related risks.	5	
			Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
1.1	Accountability and organizational structure	Principle 1: Senior Management should assign responsibility for managing technology and cyber risks to senior officers. It should also ensure an appropriate organizational structure and adequate resourcing are in place for managing technology and cyber risks across the FRFI.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			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 data and technology-related risks.	5	
1.1.1	Senior Management accountability is established	Senior Management is accountable for directing the FRFI's technology and cyber security operations and should assign clear responsibility for technology and cyber risk governance to senior officers. Examples of such roles include: Head of Information Technology; Chief Technology Officer (CTO); Chief Information Officer (CIO); Head of Cyber Security or Chief Information Security Officer (CISO). These roles should have appropriate stature and visibility throughout the institution.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			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 data and technology-related risks.	5	
			Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
			Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
			Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
			Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
			Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
			Functional	Intersects With	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
			Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
1.1.2	Appropriate structure, resources and training are provided	FRFIs should: Establish an organizational structure for managing technology and cyber risks across the institution, with clear roles and responsibilities, adequate people and financial resources, and appropriate subject-matter expertise and training; Include among its Senior Management ranks persons with sufficient understanding of technology and cyber risks; and Promote a culture of risk awareness in relation to technology and cyber risks throughout the institution. Please refer to OSFI's Corporate Governance Guideline for OSFI's expectations of FRFI Boards of Directors regarding business strategy, risk appetite and operational, business, risk and crisis management policies.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
			Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			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 cybersecurity & data protection program.	5	
			Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			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 data and technology-related risks.	5	
			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 data and technology-related risks.	5	
		Principle 2: FRFIs should define, document, approve and implement a strategic technology and cyber plan(s). The plan(s) should align to business	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.2	Technology and cyber strategy	strategy and set goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
			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 control system.	5	
1.2.1	Strategy is proactive, comprehensive and measurable	FRFI's strategic technology and cyber plan(s) should consider the following elements: Anticipate and evolve with potential changes in the FRFI's internal and external technology and cyber environment; Reference planned changes in the FRFI's technology environment; Clearly outline the drivers, opportunities, vulnerabilities, threats and measures to report on progress against strategic objectives; Include risk indicators that are defined, measured, monitored and reported on; and Articulate how technology and cyber security operations will support the overall business strategy.	Functional	Intersects With	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	
			Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
			Functional	Intersects With	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
			Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
1.3	Technology and cyber risk management framework	Principle 3: FRFIs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			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	
			Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
			Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
			Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
1.3.1	RMF is well-aligned and continuously improved	FRFIs should establish a framework for managing technology and cyber risks in alignment with its enterprise risk management framework. FRFIs should regularly review and refresh its technology and cyber RMF to make continuous improvements based on implementation, monitoring and other lessons learned (e.g., past incidents).	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
			Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			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	
			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	
			Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
			Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
			Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
			Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
1.3.2	RMF captures key elements	FRFIs should consider the following elements of risk management when establishing the technology and cyber RMF: Accountability for technology and cyber risk management, including for relevant Oversight Functions; Technology and cyber risk appetite and measurement (e.g., limits,	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	
			Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2	Technology operations and resilience	Outcome: A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable technology operations and recovery processes.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
			Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
			Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
			Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
2.1	Technology architecture	Principle 4: FRFIs should implement a technology architecture framework, with supporting processes to ensure solutions are built in line with business, technology, and security requirements.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
			Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
			Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
2.1.1	Architecture framework ensures technology supports business needs	FRFIs should establish a framework of principles necessary to govern, manage, evolve and consistently implement IT architecture across the institution in support of the enterprise's strategic technology, security and business goals and requirements.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
			Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
			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 control system.	5	
			Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
			Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
			Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
			Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
			Functional	Intersects With	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
			Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
2.1.2	Architecture is comprehensive	The scope of architecture principles should be comprehensive (e.g., considers infrastructure, applications, emerging technologies and relevant data). Using a risk-based approach, systems and associated infrastructure should be designed and implemented to achieve availability, scalability, security (Secure-by-Design) and resilience (Resilience-by-Design),	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
			Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		commensurate with business needs.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
2.2	Technology asset management	Principle 5: FRFIs should maintain an updated inventory of all technology assets supporting business processes or functions. FRFI's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
			Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
			Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
			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	
			Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
2.2.1	Technology asset management standards are established	FRFIs should establish standards and procedures to manage technology assets.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
			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	
			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	
2.2.2	Inventory is maintained and assets are categorized	FRFIs should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets owned or leased by a FRFI, and third-party assets that store or process FRFI information or provide critical business services. The asset management system, or inventory, should be supported by: Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical technology assets that are of high importance to the FRFI, or which could attract threat actors and cyber attacks, and therefore require enhanced cyber protections; and Documented interdependencies between critical technology assets, where appropriate, to enable proper change and configuration management processes, and to assist in response to security and operational incidents, including cyber attacks.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
			Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
			Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
			Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
			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	
			Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
2.2.3	Inventory records and manages technology asset configurations	The technology inventory should also include a system for recording and managing asset configurations to enhance visibility and mitigate the risk of technology outages and unauthorized activity. Processes should be in place to identify, assess, and remediate discrepancies from the approved baseline configuration, and to report on breaches.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
			Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
2.2.4	Standards for safe disposal of technology assets are established	FRFIs should define standards and implement processes to ensure the secure disposal or destruction of technology assets.	Functional	Equal	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.	10	
2.2.5	Technology currency is continuously assessed and managed	FRFIs should continuously monitor the currency of software and hardware assets used in the technology environment in support of business processes. It should proactively implement plans to mitigate and manage risks stemming from unpatched, outdated or unsupported assets and replace or upgrade assets before maintenance ceases.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
			Functional	Intersects With	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.	5	
2.3	Technology project management	Principle 6: Effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within the FRFI's risk appetite.	Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
2.3.1	Technology projects are governed by an enterprise-wide framework	Technology projects are often distinguished by their scale, required investment and importance in fulfilling the FRFI's broader strategy. As a result, they should be governed by an enterprise-wide project management framework that provides for consistent approaches and achievement of project outcomes in support of the FRFI's technology strategy. The FRFI should measure, monitor and periodically report on project performance and associated risks.	Functional	Equal	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	10	
2.4	System Development Life Cycle	Principle 7: FRFIs should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support of business objectives.	Functional	Equal	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
2.4.1	SDLC framework guides system and software development	The SDLC framework should outline processes and controls in each phase of the SDLC life cycle to achieve security and functionality, while ensuring systems and software perform as expected to support business objectives. The SDLC framework can include software development methodologies adopted by the FRFI (e.g., Agile, Waterfall).	Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
			Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
			Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity & data privacy requirements are met and that any identified risks are satisfactorily addressed.	5	
2.4.2	Security requirements are embedded throughout the SDLC	In addition to the general technology processes and controls, FRFIs should establish control gates to ensure that security requirements and expectations are embedded in each phase of the SDLC. For Agile software development methods, FRFIs should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process.	Functional	Equal	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	10	
			Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity & data privacy requirements are met and that any identified risks are satisfactorily addressed.	5	
2.4.3	Integration of development, security and technology operations	By integrating application security controls and requirements into software development and technology operations, new software and services can be delivered rapidly without compromising application security. When these practices are employed, FRFIs should ensure they are aligned with the SDLC framework and applicable technology and cyber policies and standards.	Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
			Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
			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	
			Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
			Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
2.4.4	Acquired systems and software are assessed for risk	For software and systems that are acquired, FRFIs should ensure that security risk assessments are conducted, and that systems implementation is subject to the control requirements as required by the FRFI's SDLC framework.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
			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 data and systems under review.	5	
			Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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	
			Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
2.4.5	Coding principles provide for secure and stable code	FRFIs should define and implement coding principles and best practices (e.g., secure coding, use of third-party and open-source code, coding repositories and tools, etc.).	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	8	
			Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	8	
			Functional	Intersects With	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
2.5	Change and release management	Principle 8: FRFIs should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
			Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
			Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
			Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
			Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	5	
2.5.1	Changes to technology assets are conducted in a controlled manner	FRFIs should ensure that changes to technology assets in the production environment are documented, assessed, tested, approved, implemented and verified in a controlled manner. The change and release management standard should outline the key controls required throughout the change management process. The standard should also define emergency change and control requirements to ensure that such changes are implemented in a controlled manner with adequate safeguards.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
			Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
			Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
			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	
2.5.2	Segregation of duties controls against unauthorized changes	Segregation of duties is a key control used in protecting assets from unauthorized changes. FRFIs should segregate duties in the change management process to ensure that the same person cannot develop, authorize, execute and move code or releases between production and non-production technology environments.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
			Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	5	
			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	
2.5.3	Changes to technology assets are traceable	Controls should be implemented to ensure traceability and integrity of the change record as well as the asset being changed (e.g., code, releases) in each phase of the change management process.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
2.6	Patch management	Principle 9: FRFIs should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
			Functional	Subset Of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
			Functional	Subset Of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	
2.6.1	Patches are applied in a timely and controlled manner	The patch management process should define clear roles and responsibilities for all stakeholders involved. Patching should follow the FRFI's existing change management processes, including emergency change processes. Patches should be tested before deployment to the production environment.	Functional	Subset Of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	
2.7	Incident and problem management	Principle 10: FRFIs should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
			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	
			Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
			Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
2.7.1	Incidents are managed to minimize impact on affected systems and business processes	FRFIs should define standards and implement processes for incident and problem management. Standards should provide an appropriate governance structure for timely identification and escalation of incidents, restoration and/or recovery of an affected system, and investigation and resolution of incident root causes.	Functional	Subset Of	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.	10	
			Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
2.7.2	Incident management process is clear, responsive and risk-based	FRFIs should implement processes and procedures for managing technology incidents; elements may include: Defining and documenting roles and responsibilities of relevant internal and external parties to support effective incident response; Establishing early warning indicators or triggers of system disruption (i.e., detection) that are informed by ongoing threat assessment and risk surveillance activities; Identifying and classifying incidents according to priority, based on their impacts on business services; Developing and implementing incident response procedures that mitigate the impacts of incidents, including internal and external communication actions that contain escalation and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in order to identify and remedy gaps in incident response actions and capabilities; Conducting periodic exercises and testing of incident management process, playbooks, and other response tools (e.g., coordination and communication) to validate and maintain their effectiveness; and Establishing and periodically testing incident management processes with	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
			Functional	Subset Of	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.	10	
			Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
			Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
			Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
			Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
2.7.3	Processes are established to investigate, resolve and learn from problems	FRFIs should develop problem management processes that provide for the detection, categorization, investigation and resolution of suspected incident cause(s). Processes should include post-incident reviews, root cause and impact diagnostics and identification of trends or patterns in incidents. Problem management activities and findings should inform related control processes and be used on an ongoing basis to improve incident	Functional	Equal	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	10	
			Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
2.8	Technology service measurement and monitoring	Principle 11: FRFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.	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	
			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	
			Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
2.8.1	Technology service performance is measured, monitored and regularly reviewed for improvement	FRFIs should establish technology service management standards with defined performance indicators and/or service targets that can be used to measure and monitor the delivery of technology services. Processes should also provide for remediation where targets are not being met.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
			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 cybersecurity & data privacy program.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2.8.2	Technology infrastructure performance and capacity are sufficient	FRFIs should define performance and capacity requirements with thresholds on infrastructure utilization. These requirements should be continuously monitored against defined thresholds to ensure technology performance and capacity support current and future business needs.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
			Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
			Functional	Intersects With	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.	5	
2.9	Disaster recovery	Principle 12: FRFIs should establish and maintain an Enterprise Disaster Recovery Program (EDRP) to support its ability to deliver technology services through disruption and operate within its risk tolerance.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2.9.1	Disaster recovery program is established	FRFIs should develop, implement and maintain an ERDP that sets out their approach to recovering technology services during a disruption. FRFIs should align the disaster recovery program with its business continuity management program. The EDRP should establish: Accountability and responsibility for the availability and recovery of technology services, including recovery actions; A process for identifying and analyzing technology services and key dependencies required to operate within the FRFI's risk tolerance; Plans, procedures and/or capabilities to recover technology services to an acceptable level, within an acceptable timeframe, as defined and prioritized by the FRFI; and, A policy or standard with controls for data back-up and recovery processes,	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	Intersects With	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2.9.2	Key dependencies are managed	FRFIs should manage key dependencies required to support the EDRP, such as: Information security requirements for data security and storage (e.g., encryption); and, Location of technology asset centres, backup sites, service provider locations and proximity to primary data centres, and other critical technology assets and locations. Principle 13: FRFIs should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected through disruption	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
			Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
			Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
			Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
			Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
2.9.3	Disaster recovery scenarios are tested	To promote learning, continuous improvement and technology resilience, FRFIs should regularly validate and report on their disaster recovery strategies, plans and/or capabilities against severe but plausible scenarios. These scenarios should be forward-looking and consider, where appropriate: New and emerging risks or threats; Material changes to business objectives or technologies; Situations that can lead to prolonged outage; and, Previous incident history and known technology complexities or weaknesses. FRFIs' disaster recovery scenarios should test: The FRFI's backup and recovery capabilities and processes to validate resiliency strategies, plans and actions, and confirm the organization's ability to meet pre-defined requirements; and, Critical third-party technologies and integration points with upstream and downstream dependencies, including both on- and off-premises technology.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
3	Cyber security	Outcome: A secure technology posture that maintains the confidentiality, integrity and availability of FRFIs' technology assets.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
			Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
3.0	Confidentiality, integrity and availability of technology assets is maintained	FRFIs should proactively identify, defend, detect, respond and recover from external and insider cyber security threats, events and incidents to maintain the confidentiality, integrity and availability of its technology assets.	Functional	Subset Of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	
			Functional	Intersects With	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	3	
			Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
3.1	Identify	Principle 14: FRFIs should maintain a range of practices, capabilities, processes and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
			Functional	Subset Of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			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	
			Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	
			Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
3.1.1	Security risks are identified	FRFIs should identify current or emerging cyber threats proactively using threat assessments to evaluate threats and assess security risk. This includes implementing information and cyber security threat and risk assessments, processes, and tools to cover controls at different layers of defence.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
			Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
			Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
			Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
			Functional	Subset Of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	
3.1.2	Intelligence-led threat assessment and testing is conducted	FRFIs should adopt a risk-based approach to threat assessment and testing. FRFIs should set defined triggers, and minimum frequencies, for intelligence-led threat assessments to test cyber security processes and controls. FRFIs should also regularly perform tests and exercises, to identify vulnerabilities or control gaps in its cyber security programs (e.g., penetration testing and red teaming) using an intelligence-led approach. The scope and potential	Functional	Equal	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.	10	
			Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	2	
			Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	2	
3.1.3	Vulnerabilities are identified, assessed and ranked	FRFIs should establish processes to conduct regular vulnerability assessments of its technology assets, including but not limited to network devices, systems and applications. Processes should articulate the frequency with which vulnerability scans and assessments are conducted. FRFIs should assess and rank relevant cyber vulnerabilities and threats	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	
			Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
	Data are identified, classified and	FRFIs should ensure that adequate controls are in place to identify, classify and protect structured and unstructured data based on their confidentiality classification. FRFIs should implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unauthorized access.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.4	Data are identified, classified and protected		Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
			Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
3.1.5	Continuous situational awareness and information sharing are maintained	FRFIs should maintain continuous situational awareness of the external cyber threat landscape and its threat environment as it applies to its technology assets. This could include participating in industry threat intelligence and information sharing forums and subscribing to timely and reputable threat information sources. Where feasible, FRFIs are encouraged to provide timely exchange of threat intelligence to facilitate prevention of cyber attacks, thereby contributing to its own cyber resilience and that of the broader financial sector.	Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
3.1.6	Threat modelling and hunting are conducted	Where feasible, FRFIs should maintain cyber threat models to identify cyber security threats directly facing its technology assets and services. Threats should be assessed regularly to enhance the cyber security program, capabilities and controls required to mitigate current and emerging threats. FRFIs should use manual techniques to proactively identify and isolate threats which may not be detected by automated tools (e.g., threat hunting).	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
			Functional	Subset Of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
			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	
3.1.7	Cyber awareness is promoted and tested	FRFIs should enable and encourage its employees, customers and third parties to report suspicious cyber activity, recognizing the role that each can play in preventing cyber attacks. FRFIs should create awareness of cyber attack scenarios directly targeting employees, customers and relevant third parties. In addition, the FRFI should regularly test its employees to assess their awareness of cyber threats and the effectiveness of their reporting processes and tools.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
			Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
			Functional	Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity & data privacy training that reinforce training objectives.	3	
			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	
3.1.8	Cyber risk profile is monitored and reported on	FRFIs should maintain, and report on, a current and comprehensive cyber security risk profile to facilitate oversight and timely decision-making. The profile should draw on existing internal and external risk identification and assessment sources, processes, tools and capabilities. FRFIs should also ensure that processes and tools exist to measure, monitor and aggregate residual risks.	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	
			Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
			Functional	Intersects With	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
			Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
3.2	Defend	Principle 15: FRFIs should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
			Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
3.2.1	Secure-by-design practices are adopted	FRFIs should adopt secure-by-design practices to safeguard its technology assets. Security defence controls should aim to be preventive, where feasible, and FRFIs should regularly review security use cases with a view to strengthen reliance on preventive versus detective controls. Standard security controls should be applied end-to-end, starting at the design stage, to applications, micro-services and application programming interfaces developed by the FRFI.	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
			Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
			Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
			Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	3	
3.2.2	Strong and secure cryptographic technologies are employed	FRFIs should implement and maintain strong cryptographic technologies to protect the authenticity, confidentiality and integrity of its technology assets. This includes controls for the protection of encryption keys from unauthorised access, usage and disclosure throughout the cryptographic	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
			Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.2.3	Enhanced controls and functionality are applied to protect critical and external-facing technology assets	FRFIs should employ enhanced controls and functionality to rapidly contain cyber security threats, defend its critical technology assets and remain resilient against cyber attacks by considering the following: Identifying cyber security controls required to secure its critical technology assets; Designing application controls to contain and limit the impact of a cyber attack; Implementing, monitoring and reviewing appropriate security standards, configuration baselines and security hardening requirements; and Deploying additional layers of security controls, as appropriate, to defend against cyber attacks (e.g., volumetric, low/slow network and application business logic attacks).	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
3.2.4	Cyber security controls are layered	FRFIs should implement and maintain multiple layers of cyber security controls and defend against cyber security threats at every stage of the attack life cycle (e.g., from reconnaissance and initial access to executing on objectives). FRFIs should also ensure resilience against current and emerging cyber threats by maintaining defence controls and tools. This includes ensuring continuous operational effectiveness of controls by	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	
			Functional	Subset Of	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10	
3.2.5	Data protection and loss prevention security controls are implemented	Starting with clear information classification of its data, FRFIs should design and implement risk-based controls for the protection of its data throughout its life cycle. This includes data loss prevention capabilities and controls for data at rest, data in transit and data in use.	Functional	Intersects With	Network Segmentation (macrosegementation) (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	3	
			Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	
3.2.6	Security vulnerabilities are remediated	To ensure security vulnerabilities are well managed, FRFIs should: Maintain capabilities to ensure timely risk-based patching of vulnerabilities, in vendor software and internal applications, that considers the severity of the threat and vulnerability of the exposed systems; Apply patches at the earliest opportunity, commensurate with risk and in	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
			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	
			Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
3.2.7	Identity and access management controls are implemented	FRFIs should implement risk-based identity and access controls, including Multi-Factor Authentication (MFA) and privileged access management. Where feasible, FRFIs should consider: Enforcing the principles of least privilege, conducting regular attestation of access and maintaining strong complex passwords to authenticate employee, customer and third-party access to technology assets; Implementing MFA across external-facing channels and privileged accounts (e.g., customers, employees, and third parties); Managing privileged account credentials using a secure vault; Logging and monitoring account activity as part of continuous security monitoring; Ensuring system and service accounts are securely authenticated, managed and monitored to detect unauthorized usage; and Performing appropriate background checks (where feasible) on persons granted access to the FRFI's systems or data, commensurate with the criticality and classification of the technology assets.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
			Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
			Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
			Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
			Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3	
3.2.8	Security configuration baselines are enforced and deviations are managed	FRFIs should implement approved, risk-based security configuration baselines for technology assets and security defence tools, including those provided by third parties. Where possible, security configuration baselines for different defence layers should disable settings and access by default. FRFIs should define and implement processes to manage configuration deviations.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
			Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.2.9	Application scanning and testing capabilities are employed	Where feasible, static and/or dynamic scanning and testing capabilities should be used to ensure new, and/or changes to existing, systems and applications are assessed for vulnerabilities prior to release into the production environment. Security controls should also be implemented to maintain security when development and operations practices are combined through a continuous and automated development pipeline (see paragraph 2.4.2).	Functional	Subset Of	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	10	
			Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
			Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
3.2.10	Physical access controls and processes are applied	FRFIs should define and implement physical access management controls and processes to protect network infrastructure and other technology assets from unauthorized access and environmental hazards.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
			Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.3	Detect	Principle 16: FRFIs design, implement and maintain continuous security detection capabilities to enable monitoring, alerting and forensic investigations.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			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 & data privacy-related incidents.	5	
			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	
3.3.1	Continuous, centralized security logging to support investigations	FRFIs should ensure continuous security logging for technology assets and different layers of defence tools. Central tools for aggregating, correlating and managing security event logs should enable timely log access during a cyber event investigation. For any significant cyber threat or incident, the FRFI's forensic investigation should not be limited or delayed by disaggregated, inaccessible or missing critical security event logs. FRFIs should implement minimum security log retention periods and maintain cyber security event logs to facilitate a thorough and unimpeded forensic investigation of cyber security events.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
			Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
			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	
			Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
			Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
			Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
			Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
3.3.2	Malicious and unauthorized activity is detected	FRFIs should maintain security information and event management capabilities to ensure continuous detection and alerting of malicious and unauthorized user and system activity. Where feasible, advanced behaviour-based detection and prevention methods should be used to detect user and entity behaviour anomalies, and emerging external and internal threats. The latest threat intelligence and indicators of compromise should be used to continuously enhance FRFI monitoring tools.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
			Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
			Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
			Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
3.3.3	Cyber security alerts are triaged	FRFIs should define roles and responsibilities to allow for the triage of high-risk cyber security alerts to rapidly contain and mitigate significant cyber threat events before they result in a material security incident or an operational disruption.	Functional	Subset Of	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.	10	
			Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
3.4	Respond, recover and learn	Principle 17: FRFIs should respond to, contain, recover and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.	Functional	Equal	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	10	
3.4.1	Incident response capabilities are integrated and aligned	Domain 2 sets out the foundational expectations for FRFIs' incident and problem management capabilities. FRFIs should ensure the alignment and integration between their cyber security, technology, crisis management and communication protocols. This should include capabilities to enable comprehensive and timely escalation and stakeholder coordination (internal and external) in response to a major cyber security event or incident.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
			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	
			Functional	Intersects With	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	5	
			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	
3.4.2	Cyber incident taxonomy is defined	FRFIs should clearly define and implement a cyber incident taxonomy. This taxonomy should include specific cyber and information security incident classification, such as severity, category, type and root cause. It should be designed to support the FRFI in responding to, managing and reporting on cyber security incidents.	Functional	Equal	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.	10	
3.4.3	Cyber security incident management process and tools are maintained	FRFIs should maintain a cyber security incident management process and playbooks to enable timely and effective management of cyber security incidents.	Functional	Subset Of	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.	10	
			Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
3.4.4	Timely response, containment and recovery capabilities are established	FRFIs should establish a cyber incident response team with tools and capabilities available on a continuous basis to rapidly respond, contain and recover from cyber security events and incidents that could materially impact the FRFI's technology assets, customers and other stakeholders.	Functional	Subset Of	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.	10	
			Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
3.4.5	Forensic investigations and root cause analysis are conducted, as necessary	FRFIs should conduct a forensic investigation for incidents where technology assets may have been materially exposed. For high-severity incidents, the FRFI should conduct a detailed post-incident assessment of direct and indirect impacts (financial and/or non-financial), including a root cause analysis to identify remediation actions, address the root cause and respond to lessons learned. The root cause analysis should assess threats,	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
			Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	