## NIST IR 8477-Based Set Theory Relationship Mapping (STRM) Reference Document Secure Controls Framework (SCF) version 2025.2 STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Canada OSFLB131 Focal Document URI: http://www.osfl-bait.gc.calerulguidance/subrarytechnology-cyber-risk-management Published STRM URI: http://www.osfl-bait.gc.calerulguidance/subrarytechnology-cyber-risk-management

STRM Guidance:	napus/usedirecting orangine interior	rk.com/set-theory-relationship-mapping-strm/			Published STRM URL:	intepus/social	econtrolsframework.com/content/strm/scf-strm-amaericas-canada-osfi-b13.pdf		
FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A	Purpose and scope	This Guideline settbilishe GSP's expectations related to technology and opher risk management. It is applicable to all (derivel) year/auted francois in institutions (FRFs), including foreign bank tranches and treign insurance compary tranches, to be extent it is consistent with applicable requirements and legal obligations related to their business in candad Forotnet Expectations for branches are act out in cludies E-4 on Foreign Entities Operating in Canada on a Branch Basis. These expectations all to support FRFs 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 isk", which include "tyber risk", refers to the risk arising from the inadequary, 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 toss and/or reputational damage. A "Technology asset" is something tangible (e.g., hardware, infrastructure) or infangible (e.g., software, data, information) that needs protection and supports the provision of technology encies. "Technology" (IT), and "tyber" is broadly used to include "information technology" (IT), and "tyber" is broadly used to include "information security."	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechaniama exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
Α2	Structure	This Guideline is organized into three domains. Each sets out key component of oscillation dischology and cyber risk management. 1. Governance and risk management – Sets OSFP expectations for the format accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. 2. Technology reactions and realistics – Sets OSFP's expectations for management and oversight of risks related to the design, implementation, using memory of second y assets and services. 3. Cyber security – Sets OSFP's expectations for management and services.	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	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. Technology and cyber risks are dynamic and intersect with other risk areas. FRI's should read this Guideline in conjunction with other GSH guidance, tools and supervisory communications, as well as guidance issued by other authorities applicable to the FRI's operating environment; in particular: OSH Corporate Governance Guideline: OSH Guideline E-21 (Operational Risk Management): OSH Guideline E-10 (Operational Risk Management): OSH Guideline E-21 (Operational Risk Management): OSH Technology and Opera Security (Security Risk) Rescoptized Internet Risk and stamolicalis for technology operations and Rescoptized Internet Risk and stamolicalis for technology operations and	Functional	No Relationship	NA	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 three survives.	Functional	Subset Of	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
1	Governance and risk management	frameworks. Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	Functional	Intersects With	Program 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 privecy and business executives, which meets formally and on a result basis.	5	
1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Inecuan basis. 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	
1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	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	
1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	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 enterorise-wide cybersecurity & data protection program.	5	
1	Governance and risk management	Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks. Outcome: Technology and cyber risks are governed through clear	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. Mechanisms exist to estabilish an authoritative chain of command with clear lines of	5	
1	Governance and risk management	accountabilities and structures, and comprehensive strategies and frameworks. Outcome: Technology and cyber risks are governed through clear	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	communication to remove ambiguity from individuals and teams related to managing data and technology-related risks. Mechanisms exist to develop, report and monitor cybersecurity & data privacy	5	
1	Governance and risk management	accountabilities and structures, and comprehensive strategies and frameworks.	Functional	Intersects With	Measures of Performance	GOV-05	Prechanisms exist to develop, report and monitor cydersecurity & data privacy program measures of performance. Mechanisms exist to assign one or more qualified individuals with the mission and	5	
1.1	Accountability and organizational structure	Principle 1: Senior Management should assign responsibility for managing technology and cyber lists 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 FRR.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	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	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 per FRF1 technology and option security operations and obtained assign interaperustillar for advanced assign and option and option and assign interaperustillar for advanced assign and option and and and and and and a security of the account advanced assignment and and another technology Children technology Officer (CD); Child Information Officer (CD); Hear (role at should have appropriate stature and visibility throughout the institution.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to easign once 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	
1.1.1	Senior Management accountability is established	Senior Management is accountable for directing me FRFF stechnology and cyber security perstellon and short assing clear responsibility for technology and cyber risk governance to senior differers. Examples of such rotes include: Head of Information Technology, Chill Technology Officer (CDI); Chiell Information Officer (CDI); Head of by Security or Infer Information Ecurity Officer (CDI); These roles should have appropriate stature and visibility throughout the institution.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, reposite 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 me FRFTs technology and cyber security potention and shold assing, clear responsibility for technology and cyber risk governance to senior differs. Examples of such roles include: Head of Information Technology, Chill Technology Officer (CDI); Chiell Information Officer (CDI); Head of by Security or Infert Information Exercity Officer (CDI). These roles should have appropriate stature and visibility throughout the institution.	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate opersecurity & data privacy principles into Business & Usual (BAU) practices through executive leadership involvement.	5	
1.1.1	Senior Management accountability is established	Serior Management is accountable for directing me FRFTs technology and cyber security operation and shold assign clear responsibility for technology and cyber risk governance to serior officers. Examples of technology and cyber risk governance to serior officers. Technology Officer (CD); Chief Information Officer (CD); Head of by Security or helm Information Security Officer (CD); These roles should have appropriate stature and visibility throughout the institution.	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	

version		
6/2	6/2025	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Senior Management is accountable for directing the FRFI's technology and cyber security operations and should assign clear responsibility for					Mechanisms exist to compet data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service	(optional)	
1.1.1	Senior Management accountability is established	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	Select Controls	GOV-15.1	under their control.	5	
1.1.1	Senior Management accountability is established	Serior Management is accountable for directing the FRF's technology and cyber security potentions and should assign clear responsibility for technology and cyber risk governance to serior officers. Examples of technology and cyber risk governance to serior officers. Directed wich roles include: Head of Information Technology. Officer (CDD); Chief Information Officer (CDD); Head Of Security or Ichier Information Security Officer (CDD). These roles alsold have appropriate stature and viability throughout the institution.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compet data and/or process owners to implement required cybersecurity data privacy controls for each system, application and/or service under their control.	5	
1.1.1	Senior Management accountability is established	Senior Management is accountable for directing the FRF's technology and cyber security potentions and should assign clear reaposibility for technology and cyber risk governance to senior officers. Examples of technology and cyber risk governance to senior officers. Technology Officer (CTD); Chief Information Officer (CID); Head of Lyber Security or chief Information Security Officer (CID). These roles should have appropriate stature and viability throughout the institution.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required ophersecurity data privacy controls for each system, papilication and/or service under their control are implemented correctly and are operating as intended.	5	
1.1.1	Senior Management accountability is established	Serior Management is accountable for directing the FRFTs technology and opter security operations and should assign clear responsibility for technology and cyber risk governance to serier afficient. Examples of technology and cyber risk governance to serier afficient. Samples of such roles include Head of Information Technology: Chief Technology officer (CTD); Chief Information Officer (CD); Head of Cyber Security or Chief Information Security Officer (CISO). These roles should have appropriate statum and viability throughout the institution.	Functional	Intersects With	Authorize Systems, Applications & Services	GOV-15.4	Mechaniams exist to compet data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
1.1.1	Senior Management accountability is established	Senior Management is accountable for directing the FRF's technology and cyber security operations and should assign clear responsibility for technology and cyber isk governance to senior officers. Examples of such roles include: Head of Information Technology: Chief Technology (Tofficer (CTG); Chief Information Technology: Chief Technology Chief Information Security Officer (CIS): Head Cyber Security or Chief Information Security Officer (CIS): These roles should have appropriate stature and viability throughout the institution.	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systema, applications and/or services under their control on an orgoing basis for applicable threats and risks, awlls at o ensure cybersecurity & data privacy controls are operating as intended.	5	
1.1.2	Appropriate structure, resources and training are provided	FRFBs abouds: Establish an organizational structure for managing technology and cyber risks across the institution, with clear roles and responsibilities, adequate paople and financial resources, and appropriate subject- mater expertises and training. Include samog its Serior Management ranks persons with sufficient understanding of technology and cyber risks throughout the institution. Please refer to CSF1's Corporate Governance Guideline for CSF1's Respectations of FRP. Boards of Directors regarding basiness strategy, risk popelte and operational, business, risk and crisis management	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisma exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
1.1.2	Appropriate structure, resources and training are provided	FRFIs abudi: 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- mater expertises and training. Include among its Serior 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 CSFI's Comporte Governance Guideline for CSFI's expectations of TRP Boards of Directors regarding business strategy, risk opperties and operational, business, risk and crisis management	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisme exist to coordinate cybenecurity, data protection and business alignment through a testing committee or advisory board, comprised of key cybenecurity, data privacy and business executives, which meets formally and on a regular basis.	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- mater operates 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 CSPI's Corporate Governance Guideline for CSPI's expectations of TRPI Boards of Directoria regarding busines strategy. risk appendite and operational, business, risk and crisis management PRFs should:	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisma exist to provide governance oversight reporting and recommendations to those entrustents considered material to the organization's cybersecurity & data protection program.	5	
1.1.2	Appropriate structure, resources and training are provided	Prins anoun: Establish an organizational structure for managing technology and cyber fisks across the institution, with clear roles and responsibilities, adequate people and financial resources, and appropriate subject- mater openties and training. Include among its Serior 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 CSFI's Corporate Governance Guideline for CSFI's expectations of TFR Boards of Director regrading basiness strategy, risk opperaties and operational, business, risk and crisis management	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisma exist to assign one or more qualified individuals with the mission and resources to centuly manage, cooling and the mission and enterprise-wide cybersecurity & data protection program.	5	
1.1.2	Appropriate structure, resources and training are provided	FRFBs 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- mater openites and training. Include among its Senior Management ranks persons with sufficient undentstanding of technology and cyber risks; and Promote a culture of risk warreness in relation technology and cyber risks throughout teristution. Please refet to OSFI's Comporte Governance Guideline for OSFI's Respectations of FFR Boards of Director regrading business strategy, risk popelite and operational, business, risk and crisis management	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisme exist to enforce an accountability structure so that appropriate teams and individuals are empowered, relognable and trained for mapping, measuring and managing data and technology-related risks.	5	
1.1.2	Appropriate structure, resources and training are provided	PFFIs should: Establish an organizational structure for managing technology and opter risks across the institution, with clear roles and responsibilities, adequate papple and franctic resources, and appropriate subject- mater expertises and training. Include among its Senior Hanagement rarks persons with aufficient understanding of exclusionary and roles and and Promote a culture of risk warreness in relation to technology and opter risks throughout ensittution. Please refer to CSFI's Corporate Governance Guideline for CSFI's expectation of FFR Boards of Director regarding business strategy, risk poperties and operational, business, risk and crisis management	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear times of communication tennore ambiguity from individuals and teams related to managing data and technology-related risks.	5	
1.2	Technology and cyber strategy	Principle 2: FRFIs should define, document, approve and implement a strategic technology and cyber plan(s). The plan(s) should align to business strategy and set goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment. Principle 2: FRFIs should define, document anonys and implement a	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to define the context of its business model and document the	5	
1.2	Technology and cyber strategy	Principle 2: FRFIs should define, document, approve and implement a strategic technology and cyber plan(s). The plan(s) should align to business strategy and set goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment. Businalsho 7: Beta busid #define_document_energy and environment.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	organization's mission.	5	
1.2	Technology and cyber strategy	Principle 2: FRFIs should define, document, approve and implement a strategic technology and cyber plan(). The plan(s) should align to business strategy and set goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFI's strategic technology and cyber plan(s) should consider the following elements:					Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving	(optional)	
1.2.1	Strategy is proactive, comprehensive and measurable	- 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;	Functional	Intersects With	Cybersecurity & Data Privacy Portfolio Management	PRM-01	cybersecurity & data privacy objectives.	5	
1.2.1	Strategy is proactive, comprehensive and measurable	PRF's strategic technology and cyber plan(c) should consider the following elements: Anticipate and evolve with potential changes in the FRF's internal and external technology and cyber environment; Reference planned changes in the FRF's technology environment; Cestry outline the drivers, opportunities, wiversolities, threads and measures to report on progress against strategic objectives; Include risk informs that are defined, measured, monitored and reported on; and Articulate how technology and cyber security operations will support the	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic of errecorriy & data privacy-specific business plan and set of objectives to achieve that plan.	5	
1.2.1	Strategy is proactive, comprehensive and measurable	Prior strategic checknology and cyber plan(i) should consider the tollowing elements: Anticipate and evolve with potential changes in the FRP's internal and external technology and cyber environment; Reference planned changes in the FRP's technology environment; Ceatry outline horizer, opportunities, winershillines, the sta and measures to report on progress against strategic objectives; Include risk indicators that are definer, measured, monitored and reported on, and Articulate how technology and cyber security operations will support the	Functional	Intersects With	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	5	
1.2.1	Strategy is proactive, comprehensive and measurable	Insert Insteam a rotation. FRP's strategic technology and cyber plan(s) should consider the following elements: Anticipate and evolve with potential changes in the FRF's internal and acternal technology and cyber environment; Reference planned changes in the FRF's technology environment; Ceatry outline the drivers, opportunities, winershillens, threats and measures to report on progress against strategic objectives; Include risk indicators that are definer, measured, monitored and reported on, and Articulate how technology and cyber security operations will support the	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	
1.2.1	Strategy is proactive, comprehensive and measurable	Jourcel have an extension of the second or share plan(s) should consider the tollowing elements: Anticipate and evolve with potential changes in the FRF's internal and external technology and cyber environment; Reference planned changes in the FRF's technology environment; Celarly outline the drivers, opportunities, whereholdings, threats and measures to report on progress against strategic objectives; Include risk indicators that are definer, measured, monitored and reported or, and Articulate how technology and cyber security operations will support the	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	
1.2.1	Strategy is proactive, comprehensive and measurable	FRFT's strategic technology and cyber plan(s) should consider the following elements: chickpate and evolve with potential changes in the FRFT's internal and external technology and cyber environment; Reference planned changes in the FRFT's technology environment; Cesiny outline the drawn, opportunity, witherabilities, threats and measures to export on progress against strategic chickness, threats and measures to export on progress against strategic chickness deported on use that are defined, measured, monitored and apportation are strated.	Functional	Intersects With	Cybersecurity & Data Privacy in Project Management	PRM-04	Nechanisms exist to assess ophemecoully & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
1.2.1	Strategy is proactive, comprehensive and measurable	FRFF is 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 tanges in the FRFI's technology environment; Castry outline the drivers, opportunities, withersibilies, these and measures to ropeo ropeoses agained strategic objectives; Include risk indicators that are defined, measured, monitored and reported or, and Miticulate how technology and cyber security operations will support the measure to ropeose	Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisma exist to identify critical system components and functions by performing a critically analysis for critical systems, system components or services at pre-defined decision points in the Secure Development LIfe Cycle (SDLC).	5	
1.2.1	Strategy is proactive, comprehensive and measurable	FRFT's attralegic 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 thanges in the FRFI's technology environment; Castro cultine the drivers, opportunities, winersbillies, thesas and measures to roper on progress against strategic objectives; Include risk indicators that are defined, measured, monitored and reported or; and Articulate how technology and cyber security operations will support the meaned to be technology.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisme exist to define business processes with consideration for cybersecurity & data privacy bird determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and reginizations; and (2) Information protection needs arising from the defined business processes and reviews 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	
1.3	Technology and cyber risk management framework	Principle 3: FRFIs aboutd establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define FRF1s processes and requirements to identify, assess, manage, monitor and report on technology and cyber 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 effecting 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	
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 RFFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber and more table.	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	
1.3	Technology and cyber risk management framework	technology and cyber risks. Principies : FTFs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and defines FRF's processes and requirements to identify, assess, manage, monitor and report on	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1.3	Technology and cyber risk management framework	technology and cyber risks. Principies 3: FFIS 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 RFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber and more fails	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	
1.3	Technology and cyber risk management framework	technology and cyber risks. Principle 3: FRFs should estabilish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define FRF's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.	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	Technology and use many manework for managing technology and cyber risks in alignment with its entreprise risk management framework. FRFIs should regularly releval 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	

version		
6/2	6/2025	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should establish a framework for managing technology and cyber	Rationate	Relationship			Mechanisms exist to coordinate cybersecurity, data protection and business	(optional)	
1.3.1	RMF is well-aligned and continuously improved	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	Steering Committee & Program Oversight	GOV-01.1	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	
1.3.1	RMF is well-aligned and continuously improved	FRFs 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	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, a planned interval or it inginiterant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1.3.1	RMF is well-aligned and continuously improved	FRFs should establish a framework for managing technology and cyber risks in alignment with its enterprise risk management framework. FRFs should regularly review and refresh its technology and cyber MMF to make continuous improvements based on implementation, monitoring and other lessons learned (e.g., past incidents).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechaniama exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
1.3.1	RMF is well-aligned and continuously improved	FRFIs should establish a framework for manging 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	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 miligation actions.	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	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	
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	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and factical risk management controls.	10	
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	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	
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	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Aechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	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	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecyclas of technology assets.	5	
1.3.2	RMF captures key elements	stabilishing the technology and cyber RMF: Accountability for technology and cyber risk management, including for relevant Oversight Functions: Tachnology and cyber risk taxonomy: Control domains for technology and cyber security: Policies, standards and processes governing technology and cyber risk hich are approved, regularly reviewed and consistently implemented enterprise-wide; Processes to risk dentifying, assessing, managing, monotroing and reporting on technology and cyber risks, including processes for managing exceptions; Management of unique risks poled by emerging threats and technologics; and Reporting to Sanior Management on technology and cyber risk appette ensearurse, programs and tends to inform the FRFI's current and emerging risk profile. Please refet to SSTI's Corporato Coversance Guideline for SST's sepectations in relation to FRFI Oversight Functions, which include Risk	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechaniame exist to develop a security Concept of Operations (COMOS), or a similarly-defined pain for a alreiving operaeurity objections, that documenta management, operational and technical measures implemented to apply defense-in- depth techniques that is communicated to all appropriate stakeholders.	5	
1.3.2	RMF captures key elements	FRFIs isolud consider the following elements of risk management when estabilishing the technology and cyber RMF: Accountability for 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, thresholds and toler risk appetite and measurement (e.g., limits, thresholds and toler risk appetite and measurement (e.g., limits, thresholds and toler risk appetite and measurement (e.g., limits, thresholds, and toler risk appetite and measurement (e.g., limits, which are approved, regularly reviewed and consistently implemented enterprise-wide, prevised, regularly reviewed and consistently implemented in technology and cyber risk, posed by emerging threats and technologies; and Reporting to Senior Management on technology and cyber risk appetite measures, exposures and trench to inform the FRPYs current and emerging risk profile.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisma 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	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	
2	Technology operations and resilience	sustainable technology operations and recovery processes. Outcome: A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable tocheclogy operations and recovery processes.	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,	5	
2	Technology operations and resilience	sustainable technology operations and recovery processes. Outcome: A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	implementation and modification of systems and services. Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
2	Technology operations and resilience	sustainable technology operations and recovery processes. 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. Principle 4: FRFIs should implement a technology architecture	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. Mechanisms exist to define business processes with consideration for cybersecurity	5	
2.1	Technology architecture	Principle 4: FRPIs should implement a technology architecture framework, with sporting processes to smare solution 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 privery build determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and a state of the stat	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	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	
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	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 building and building and provide the strategic technology.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
2.1.1	Architecture framework ensures technology supports business needs	and business goals and requirements. 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	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	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 coals and requirements.	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	

version	2025.2
6/2	6/2025

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
	Architecture framework ensures	FRFIs should establish a framework of principles necessary to govern,			Operationalizing		Mechanisms exist to compel data and/or process owners to operationalize	(optional)	
2.1.1	technology supports business needs	manage, evolve and consistently implement IT architecture across the institution in support of the enterprise's strategic technology, security and business coals and reouirements. FRFIs should establish a framework of principles necessary to govern,	Functional	Intersects With	Cybersecurity & Data Protection Practices	GOV-15	cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
2.1.1	Architecture framework ensures technology supports business needs	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	Select Controls	GOV-15.1	cybersecurity & data privacy controls for each system, application and/or service under their control.	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	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	
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	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	
2.1.1	Architecture framework ensures technology supports business	and business coals and recuirements. 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	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	
2.1.1	needs Architecture framework ensures technology supports business	and business coals and requirements. 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	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	5	
2.1.2	needs Architecture is comprehensive	and butiness costs and requirements. The scoped architecture principles should be comprehensive (e.g., considers infrastructure, applications, emerging technologies and relevant das). Using a risk-based approach, systems and associated infrastructure should be designed and millemented to achive availability, scalability, security (Secure by-Design) and realience (Resilience-by-Design), commensustate with business needs.	Functional	Intersects With	Secure Engineering Principles	SEA-01	operating as intended. Mechanisms exist for a localitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
2.1.2	Architecture is comprehensive	The scope of architecture principles should be comprehensive (e.g., consider infrastructure, applications, emerging technologies and relevant data). Using a risk-based approach, systems and associated infrastructure should be designed and implemented to achieve availability, security (Becure by-Design) and resilience (Resilience-by-Design), commensustate with basiness needs.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
2.1.2	Architecture is comprehensive	The scope of architecture principles should be comprehensive (e.g., consider infrastructure, applications, emerging technologies and relevant das). Using a risk-based approach, systems and associated infrastructure should be designed and implemented to achieve availability, acativity Secure D-Design) and realisece (Resilience by-Design), 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 adresses 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 of functions. FRFI's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to manue asset integrity, provide of the safe disposal of assets at the end of their Ulle cycle, and monitor and manage technology currency.	Functional	Intersects With	Asset Governance	AST-01	Mechaniams exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
2.2	Technology asset management	Principle 5: FRFIs should maintain an updated inventory of all technology assets supporting business processes of functions. FRF's asset management processes should adverse classification of assets to facilitate risk identification and assessment, record configurations to ensure asset lineity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency.	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	
2.2	Technology asset management	Principle's FFRIs should maintain an updited inventory of all technology assess supporting burness processes for forcions. FRFIs asset management processes should address classification of assets to facilitate risk identification and assessment, record onfigurations to ensure asset integrity, provide for the address data states at the end of their ille cycle, and monitor and manage technology currency.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately relates the current optimum, applications and services in use; (2) identifies authorized software products, including business justification details; (3) is at the tevel of ganularity deemed necessary for tracking and reporting; (4) includes organization defined intramation deemed necessary to achieve effective property accountability; and (5) is available for review and audit by designated organizational personnel.	5	
2.2	Technology asset management	Principle 5: FRPIs should maintain an updated inventory of all technology assets supporting business processes or functions. FRPT's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity provide of the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency.	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	
2.2	Technology asset management	Principle's FRRIs should maintain an updated inventory of all technology assets supporting buildness processes for functions. FRR's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide of the safe classical assets at the end of their life cycle, and monitor and manage technology currency.	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	
2.2.1	Technology asset management standards are established	FRFIs should establish standards and procedures to manage technology assets.	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	
2.2.1	Technology asset management standards are established	FRFIs should establish standards and procedures to manage technology assets.	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 socieffic socials of the process area.	5	
222	Inventory is maintained and assets are categorized	PRHs should maintine ocument and compehensive asset management system, or inventory, that catalogue stechology assets throughout their tile cycle. Based on the FRF1 risk tolerance, this may include assets owned or leased by a FRF1, and thick party assets that store or process FRF1 information or provide ortical 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 is the FRF1 or which could attract threat actors and opeer attacks, and therefore require enhanced Documents interdependencies between critical technology assets, where approprints, including cyber change and configuration management processes, include to size attacks.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to localize an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
222	Inventory is maintained and assets are categorized	FRFs about maintain a current and compehensive asset management system, or inventory, mat catalogues technology assets throughout their tille cycle. Based on the FRF1 raik tudennon, this may include assets nonend or lease by a FRF, and thick party assets that also ere process FRFI information or provide critical husiness services. The asset management system, or inventory, should be supported by: Processes to categorise the chnology assets based on their criticality and/or classification. These processes inoud identify critical technology assets that are of high importance to the FRFI, or which could attact threat acoust and cyber attacks, and therefore require enhanced cyber protections; and therefore negative management processes, and to assist in response to acoutly and operational incidents, including cyber attacks.	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	

version 2025.2	
6/26/2025	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should maintain a current and comprehensive asset management					Mechanisms exist to perform inventories of technology assets that:	(optional)	
		system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets					<ol> <li>Accurately reflects the current systems, applications and services in use;</li> <li>Identifies authorized software products, including business justification details;</li> </ol>		
		owned or leased by a FRFI, and third-party assets that store or process					(3) Is at the level of granularity deemed necessary for tracking and reporting;		
		FRFI information or provide critical business services. The asset management system, or inventory, should be supported by:					<ul> <li>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and</li> </ul>		
							(5) Is available for review and audit by designated organizational personnel.		
2.2.2	Inventory is maintained and assets are categorized	Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical	Functional	Intersects With	Asset Inventories	AST-02		5	
		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.							
-		FRFIs should maintain a current and comprehensive asset management					Mechanisms exist to identify and document the critical systems, applications and		
		system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets					services that support essential missions and business functions.		
		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							
2.2.2	Inventory is maintained and assets are categorized	and/or classification. These processes should identify critical	Functional	Intersects With	Identify Critical Assets	BCD-02		5	
	_	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.							
		FRFIs should maintain a current and comprehensive asset management					Mechanisms exist to ensure data and assets are categorized in accordance with		
		system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets					applicable statutory, regulatory and contractual requirements.		
		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:							
2.2.2	Inventory is maintained and assets are categorized	Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical	Functional	Intersects With	Data & Asset Classification	DCH-02		5	
	are earegonzed	technology assets that are of high importance to the FRFI, or which could attract threat actors and cyber attacks, and therefore require enhanced			UUUUUU				
		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.							
		FRFIs should maintain a current and comprehensive asset management					Mechanisms exist to maintain inventory logs of all sensitive media and conduct		
1		system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets					sensitive media inventories at least annually.		
		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:							
2.2.2	Inventory is maintained and assets are categorized	Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2		5	
		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.							
		The technology inventory should also include a system for recording and					Mechanisms exist to perform inventories of technology assets that:		
		managing asset configurations to enhance visibility and mitigate the risk of technology outages and unauthorized activity. Processes should be in					<ol> <li>Accurately reflects the current systems, applications and services in use;</li> <li>Identifies authorized software products, including business justification details;</li> </ol>		
2.2.3	Inventory records and manages	place to identify, assess, and remediate discrepancies from the	Functional	Intersects With	Asset Inventories	AST-02	(3) Is at the level of granularity deemed necessary for tracking and reporting;	5	
	technology asset configurations	approved baseline configuration, and to report on breaches.					<ul> <li>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and</li> </ul>		
							(5) Is available for review and audit by designated organizational personnel.		
		The technology inventory should also include a system for recording and managing asset configurations to enhance visibility and mitigate the risk			Overfine		Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific		
2.2.3	Inventory records and manages	of technology outages and unauthorized activity. Processes should be in	Functional	Intersects With	Configuration Management Database	AST-02.9	information.	5	
	technology asset configurations	place to identify, assess, and remediate discrepancies from the approved baseline configuration, and to report on breaches.			(CMDB)				
	Standards for safe disposal of	FRFIs should define standards and implement processes to ensure the			Secure Disposal,		Mechanisms exist to securely dispose of, destroy or repurpose system components		
2.2.4	technology assets are established	secure disposal or destruction of technology assets.	Functional	Equal	Destruction or Re-Use of Equipment	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	10	
	established	FRFIs should continuously monitor the currency of software and			Equipment		recovered from these components. Mechanisms exist to manage the usable lifecycles of technology assets.		
2.2.5	Technology currency is continuously assessed and	hardware assets used in the technology environment in support of business processes. It should proactively implement plans to mitigate	Functional	Intersects With	Technology Lifecycle	SEA-07.1		5	
2.2.0	continuously assessed and managed	and manage risks stemming from unpatched, outdated or unsupported assets and replace or upgrade assets before maintenance ceases.	runctionat	ALCONCESS WITH	Management	3EP-07.1		Å	
L									
	Technology currency is	FRFIs should continuously monitor the currency of software and hardware assets used in the technology environment in support of					Mechanisms exist to prevent unsupported systems by: (1) Replacing systems when support for the components is no longer available from		
2.2.5	continuously assessed and	business processes. It should proactively implement plans to mitigate and manage risks stemming from unpatched, outdated or unsupported	Functional	Intersects With	Unsupported Systems	TDA-17	the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of	5	
	managed	assets and replace or upgrade assets before maintenance ceases.					unsupported system components required to satisfy mission/business needs.		
-		Principle 6: Effective processes are in place to govern and manage			Cybersecurity & Data		Mechanisms exist to assess cybersecurity & data privacy controls in system project		
2.3	Technology project management	technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within	Functional	Intersects With	Privacy In Project	PRM-04	development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to	5	
	-	the FRFI's risk appetite. Principle 6: Effective processes are in place to govern and manage			Management		meeting the requirements. Mechanisms exist to identify critical system components and functions by		
2.3	Technology project	technology projects, from initiation to closure, to ensure that project	Functional	Intersects With	Cybersecurity & Data Privacy Requirements	PRM-05	performing a criticality analysis for critical systems, system components or services	5	
	management	outcomes are aligned with business objectives and are achieved within the FRFI's risk appetite.			Definition		at pre-defined decision points in the Secure Development Life Cycle (SDLC).		
		Principle 6: Effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project					Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:		
2.3	Technology project	outcomes are aligned with business objectives and are achieved within	Functional	Intersects With	Business Process	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other	5	
2.0	management	the FRFI's risk appetite.	- ancoonat	microcold With	Definition		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.		
		Technology projects are often distinguished by their scale, required investment and importance in fulfilling the FRFI's broader strategy. As a					Mechanisms exist to assess cybersecurity & data privacy controls in system project		
	Technology projects are	result, they should be governed by an enterprise-wide project		_	Cybersecurity & Data		development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to		
2.3.1	governed by an enterprise-wide framework	management framework that provides for consistent approaches and achievement of project outcomes in support of the FRFI's technology	Functional	Equal	Privacy In Project Management	PRM-04	meeting the requirements.	10	
		strategy. The FRFI should measure, monitor and periodically report on project performance and associated risks							
		Principle 7: FRFIs should implement a System Development Life Cycle			Secure Development Life		Mechanisms exist to ensure changes to systems within the Secure Development Life		
2.4	System Development Life Cycle	SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support	Functional	Equal	Cycle (SDLC)	PRM-07	Cycle (SDLC) are controlled through formal change control procedures.	10	
		of business objectives. The SDLC framework should outline processes and controls in each			Management		Mechanisms exist to assess cybersecurity & data privacy controls in system project		
	PDI C fromours to a lides a	phase of the SDLC life cycle to achieve security and functionality, while			Cybersecurity & Data		development to determine the extent to which the controls are implemented		
2.4.1	SDLC framework guides system and software development	objectives. The SDLC framework can include software development	Functional	Intersects With	Privacy In Project Management	PRM-04	correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
		methodologies adopted by the FRFI (e.g., Agile, Waterfall).			ariagen lefti				
		The SDLC framework should outline processes and controls in each phase of the SDLC life cycle to achieve security and functionality, while	-				Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services		
2.4.1	SDLC framework guides system	ensuring systems and software perform as expected to support business	Functional	Intersects With	Cybersecurity & Data Privacy Requirements	PRM-05	performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
1	and software development	objectives. The SDLC framework can include software development methodologies adopted by the FRFI (e.g., Agile, Waterfall).			Definition				
		1		1	1	1	i la	1	

version 2025.2	
6/26/2025	

FDE #	FDE Name	Focsl Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		The SDLC framework should outline processes and controls in each phase of the SDLC life cycle to achieve security and functionality, while provide a partore and optimum professor as associated to expend the unport the unique provided and the security of the security					Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:	(optional)	
2.4.1	SDLC framework guides system and software development	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	Business Process Definition	PRM-06	(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 initialized.	5	
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 cyclot caberieve 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., Agle, Waterfall).	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechaniams exist to ensure changes to systems within the Secure Dewelopment Life Cycle (SDLC) are controlled through formal change control procedures.	5	
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 FRF (e.g. Agie, Waterfall).	Functional	Intersects With	Software Design Review	TDA-06.5	Machaniams 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	the necessary SDLC and security-by-design principles throughout its	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	
2.4.2	Security requirements are embedded throughout the SDLC	Aeila noncess 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 Aeile process.	Functional	Intersects With	Software Design Review	TDA-06.5	Machaniams 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	Anim process. By integrating application security controls and requirements into software development and technology operations, new software and services can be delivered najidi without compromising application security. When these practices are employed, FRFIs should ensure they are aligned with the SDLC transevork and applicable technology and coher opolises 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	
2.4.3	Integration of development, security and technology operations	The notates and additional 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 SUC framework and applicable technology and cyber policies and standards.	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 aganizational 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	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 transevork and applicable technology and rober prolises and transforms.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	obtibilited Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	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 transevork and applicable technology and rober notices and transforms.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisme exist to facilitate the implementation of tailored development and acquisition attractiges, contract tools and procurement methods to meet unique business needs.	5	
2.4.3	Integration of development, security and technology operations	By integrating application security controls and requirements into software development and technology pertainsn, new software and services can be delivered rapidly without compromising application eacurity. 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	Product Management	TDA-01.1	Machaniams exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with explicable statutory, regulatory and/or contractual obligations.	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, FRIs should ensure they are aligned with the SDLC transvork and applicable technology and rober prolises and transforms.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Alccharisme exist to require software developers to ensure that their software development processes entployinguiver-resognized secure practices for necure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or matformed 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 FRP'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	
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	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	
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	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybensecurity & data privacy controls in systems, applications and services through information Assurance Program (AP) 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	
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	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. Mechanisms exist to develop andications based on Secure Software Development	8	
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	Secure Software Development Practices (SSDP)	TDA-06	Prechanisms exist to develop applications based on Secure Soltware Development Practices (SSDP). Mechanisms exist to require the developer of the system, system component or	8	
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.). Principle S: FRFIs should establish and implement a technology change	Functional	Intersects With	Criticality Analysis	TDA-06.1	Mechanisma 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 Cvcle (SDLC). Mechanisms exist to facilitate the implementation of a change management	5	
2.5	Change and release management	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	program.	5	
2.5	Change and release management	Principle 8: FRFs 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	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	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 change to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	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	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	
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 change to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.	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	PRFs houdd ensure that changes to technology assets in the production invinciment at an elevanetical, suscess the technology assets and the production inplanemental and verified in a controlled manner. The change and relates management standard should unlime he key controls required throughout the change management process. The standard should also define emergency change and control sugmerners to ensure that such changes are implemented in a controlled manner with adequate adeauants.	Functional	Intersects With	Change Management Program	CHG-01	Machanitams exist to facilitate the implementation of a change management program.	5	
2.5.1	Changes to technology assets are conducted in a controlled manner	FRFs hould ensure that changes to technology assets in the production environment are documented, assessed, tested, approved, implemented and verified in controlled manner. The change and release management standard should allow lime the key control to neguried throughout the change management process. The standard should also define emergency change and control equirements to ensure that such changes are implemented in a controlled manner with adequate wheneverts.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should ensure that changes to technology assets in the production	Rationate	Relationship			Mechanisms exist to prohibit unauthorized changes, unless organization-approved	(optional)	
2.5.1	Changes to technology assets are conducted in a controlled manner	environment are documented, assessed, testad, 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 setements.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	change requests are received.	5	
2.5.1	Changes to technology assets are conducted in a controlled manner	FIPTs haloud ensure that changes to technology assets in the production environment at ordourmentor, assessed, steted, approved, implemented and verified in a controlled manner. The change and release management traductar should outline the key controls required throughout the change management process. The standard should also define emergency change and control equirements to ensure that such changes are implemented in a controlled manner with adequate adminute.	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	
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	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	5	
2.5.2	Segregation of duties controls against unauthorized changes	Segregation of duties is a key control used in protecting assets from unsufficized changes. FRPIs 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-modulution technology environments. Controls should be implemented to ensure traceability and integrity of	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechaniams 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	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 Vulnerability & Patch	CHG-02	Mechanisms exist to facilitate the implementation and monitoring of vulnerability	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	Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the imprementation and monitoring of vulnerability management controls. Mechanisms exist to ensure that vulnerabilities are property identified, tracked and	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. Principle 9: FRFIs should implement patch management processes to	Functional	Subset Of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. Mechanisms exist to conduct software patching for all deployed operating systems,	10	
2.6	Patch management	Principle 2: FKH's should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws. The patch management process should define clear roles and	Functional	Subset Of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware. Mechanisms exist to conduct software patching for all deployed operating systems,	10	
2.6.1	Patches are applied in a timely and controlled manner	responsibilities for all stakeholders involved. Patching should follow the FRF's existing change management processes, including emergency change processes. Patches should be tested before deployment to the roduction environment.	Functional	Subset Of	Software & Firmware Patching	VPM-05	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. Principle 10: FRFIs should effectively detect, log, manage, resolve,	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to tacilitate an organization-wide response capability for cybersecurity & data privacy- related incidents. Mechanisms exist to cover:	10	
2.7	Incident and problem management	monitor and report on technology incidents and minimize their impacts.	Functional	Intersects With	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (2) Analysis; (4) Constimment; (5) Eradication; and Bi Recovery	5	
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	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	
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	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	FPTBs blockuld define standards and implement processes for incident and problem management. Standards houd 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) Peparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (5) Bencover.	10	
2.7.1	Incidents are managed to minimize impact on affected systems and business processes	FRFs 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 investization and resolution of incident root causes.	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	FRFBs hould 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 affective incident response; Establishing agely avaming includents or uriges of system disruption (i.e., detection) that are informed by ongoing threat assessment and risk survailtance activities; Identifying and classifying incident seconding to priority, based on their impacts on business services; Developing and implementing incident response procedures that mitigate the impacts of indicets, including internal and external communication actions that contain escalation and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in accento identify and remedy ages in incident response actions and capabilities. Conducting periodic testing and incident management process, playbooks, and other response tools lea; conordination and Establishing and periodically testing incident management process, playbooks, and other response tools lea; conordination and Establishing and periodically testing incident management process. Julybooks, and other response tools lea; conordination and Establishing and periodically testing incident management process. Julybooks, and other response tools lea; conordination and Establishing and periodically testing incident management process. Julybooks and other plausible scenarios set this hird parties.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to incluitate an organization-wide response capability for cybersecurity & data privacy- related incidents.	10	
2.7.2	Incident management process is clear, responsive and risk- based	technology incidents; elements may include: Defining and documenting roles and responsibilities of relevant internal de destrand particles to support effective incident response Establishing early warning inclusion: or trigger of system disruption (i.e., detector) hat are informed by ongoing threat assessment and risk surveillance activities; Litabilishing early warning inclusions according to priority, based on their impacts on business services; Developing and implementing inclusions exposite response procedures that miligite the impacts of inclusions, including internal and external communications actions that contain escalation and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in order to identify and remedy ago in incident response actions and communication activa, and other response tools (e.g., condition) and communication is enricidually testing incident management process, playbook, and other response tools (e.g., condition and communication) to validate and maintain their effectiveness; and Establishing and procidually testing incident management processes with third parties.	Functional	Subset Of	Incident Handling	IRO-02	(1) Preparation: (2) Automated event detection or manual incident report intaka; (3) Analysis: (4) Containment; (8) Eradication; and (8) Recovery.	10	

8 of 17

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should implement processes and procedures for managing technology incidents; elements may include:	Rationale	Relationship			Control Description Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	(optional)	
2.7.2	Incident management process is clear, responsive and risk- based	Becimiogy inclusions, elements may incluse: Defining and documenting roles and responsibilities of relevant internal and external parties to support affective incident response; Establishing and carbo warming incidence or stigges of system disruption (i.e., detection) that are isformed by ongoing threat assessment and risk warvalitance activities; Identifying and classifying incident seconding to priority, based on their impacts on business envices: Developing and implementing incident response procedures that mitigate the impacts of indicents, including internal and external communication actions that contain escalation and notification triggers and processes; Parforming periodic testing and incident response actions and capabilities; Conducting periodic testing and incident response actions and capabilities;	Functional	Intersects With	Indicators of Compromise (ICC)	IRO-03	agris of polential cytorisecurity events.	5	
27.2	Incident management process is clear, responsive and risk- based	PFIFs 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 avaming includent or signes of system disruption (i.e., detection) that are informed by ongoing threat assessment and risk surveillance activities; Usentbying and classifying incident response procedures that minipate the impacts of indivers, incident response procedures that minipate the impacts of indivers, incident response procedures that minipate the impacts of indivers, incident response external communication actions that contain exclusion and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in acter to lentify and enterely gaps in incident traggers each process, pubpolos, and other response tools leg_, coordination and capabilities; Conducting periodic exercises and testing of incident management process, pubpolos, and other response tools leg_, coordination and Establishing and periodically testing incident management process. pubpolos, and other response tools leg, coordination and Establishing and periodically testing incident management process. pubpolos, and other sponse tools leg with the paties.	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	
		FRFIs should implement processes and procedures for managing technology incidents; elements may include:					Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.		
27.2	Incident management process is clear, responsive and risk- based	Defining and documenting roles and responsibilities of relevant internal and external parties to support effective incident response; Establishing early avaming indications or trigger of system disruption (i.e., detection) that are informed by ongoing threat assessment and risk availations activities; Identifying and classifying incident secording to priority, based on their impacts on business services; Developing and implementing incident response procedures that militgate the impacts of indicents, incident response actual communication actions that contain escalation and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in conducting periodic testing and exercises using plausible scenarios in conducting periodic testing and exercises using plausible scenarios in process, platybooks, and other response tools (e.g., coordination and communication) actualides and mattain their effectiveness; and Establishing and periodical busing incident management process, bitybooks, and other using and services and the bitybooks and other seponse tools (e.g., coordination and cettablishing and periodical busing incident management process, with hird particle busing incident management process.	Functional	Intersects With	Incident Response Testing	IRO-06		5	
		FRFIs should implement processes and procedures for managing technology incidents; elements may include:					Mechanisms exist to establish an integrated team of cybersecurity. IT and business function representatives that are capable of addressing cybersecurity & data privacy		
27.2	Incident management process is clear, responsive and risk- based	Defining and documenting roles and responsibilities of relevant internal and external parties to support effective incident response; Establishing early avaming indicators or trigger of system disruption (i.e., detection) that are informed by orgoing threat assessment and risk availlance activities; Identifying and classifying incident secording to priority, based on their impacts on business services; Developing and implementing incident response procedures that mitigate the impacts of indicets, incident response derivation triggers and processes; Performing periodic testing and exercises using plausible scenarios and constructions actions that contain escalation and notification triggers and processes; Performing periodic testing and exercises using plausible scenarios in conducting periodic testing and exercises using plausible scenarios in process, playbooks, and other response tools (e.g., coordination and cathabilities; Conducting and periodical testing of incident management process, playbooks, and other seponse tools (e.g., coordination and cathabilities; Conducting and periodical testing incident management process, playbooks, and other seponse tools (e.g., coordination and cathabilities; Conducting and periodical testing incident management process, with hird particular testing incident management process, with hird particular testing prioridical testing and periodical testing and periodical testing of incident management process with hird particular testing prioridical testing periodical testing perioding te	Functional	Intersects With	Integrated Security Incident Response Team ((SIRT)	IRO-07	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 inclorent cause(s), rocesses should include posi-inclident reviews, root cause and impact diagnostica and identification of trends or pattern in inclidents. Problem management activities and findings abuild inform related control processes and be used on an ongoing basis to improve inclident management processes and procedures, including change and relases management.	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	
2.7.3	Processes are established to investigate, resolve and learn from problems	FRIs about develop problem management processes that provide for the detection, categorization, investigation and resolution of suspected indicated cause(s), torcesses should include post-incident reviews, root cause and impact diagnostica and identification of trends or patterns in incidents. Problem management activities and findings should inform related control processes and procedures, including basis to improve incident management processes and procedures, including change and release management.	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 hundress aceds 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 /	5	
2.8	Technology service measurement and monitoring	business meds are met. Principle 11: FBFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met. Principle 11: FBFIs should develop service and capacity standards and	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	assigned tasks. 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 spacefic goals of the arccess area. Mechanisms exist to derify pricing system components and functions by	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	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	
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	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	FFFIs should establish technology service management standards with defined performance indicators and/or service target that can be used to measure and monitor the delivery of technology services. Processes should also provide for mendiation 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	
2.8.1	Technology service performance is measured, monitored and regularly reviewed for improvement	FRFs 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	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (RPIs) to assist organisational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	

version	2025.2
6/2	6/2025

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
	Technology infrastructure	FRFIs should define performance and capacity requirements with thresholds on infrastructure utilization. These requirements should be					Mechanisms exist to facilitate the implementation of capacity management controls to ansure ontimal system performance to meet expected and enticipated future.	(optional)	
2.8.2	Technology infrastructure performance and capacity are sufficient	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	to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
2.8.2	Technology infrastructure performance and capacity are sufficient	FRFs 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 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	
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	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	
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	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	FIFIs should develop, implement and maintain an EDDP that sets out betra approach to covering technology services during disruption. FIFIs should align the disaster recovery program with its business continuity management program. The EDDP 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 FIFI's risk tolerance; Plans, procedures and/or capabilities to recover technology services and acceptable level, within an acceptable level, within an acceptable level, within an acceptable level with on more capabilities to drata back-up and recovery	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisma exist to facilitate the implementation of contingency planning controls to help ensure realisent assets and services (e.g., Continuity of Operations Pfan (COOP) or business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
2.9.1	Disaster recovery program is established	processes, requirements for data storage and periodic testing, FRFIs should develop, implement and maintain an ERDP that sets out their approach to recovering technologie services during disruption. FRFIs should align the disaster recovery program with its business continuity management program. The ERPP 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 sick tolerance; Plans, procedure and/or capabilities to recover technology services to an acceptable level, within an acceptable timeframe, as defined and prioritize by the FRFI; and, A policy or standard with controls for data back-up and recovery processes, requirements for data back-up and recovery	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	PRFs hould develop, implement and maintain an EEDP that sets out that approach to recovering technology services during a disruption. PRFs should align the disaster recovery program with its business continuity management program. The EDRP about detablish: Accountability management program. The BORP about detablish: Accountability management program. The BORP about detablish: Accountability management program with the services and key dependencies required to operate within the FRFs risk tolerance. Pana, procedure and/or capabilities recover pacifications an acceptable level, within an acceptable timeframe, as defined and protesses to relevances to recover technologi services to an acceptable level, within an acceptable timeframe, as defined and protesses, requirements for data back-up and recovery processes, requirements for data back-up and recovery	Functional	Intersects With	Recovery Operations Criteria	BCD-01.5	Aschartame exist to define opecific orteris that must be met to initiate Business Continuity / Disaster Reacover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Dijectives (RTDs) and Recovery Point Objectives (RPOs).	5	
2.9.1	Disaster recovery program is established	FRIPs should develop, implement and maintain an ERDP that sets out their approach to recovering technology services during a disruption. FRIPs should align the disaster recovery program with its business continuity management program. The ERRP 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 around to operate within the FRIP in tak technology services han 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, requirements for data back-up and recovery processes, requirements for data back-up and recovery processes.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as wrift 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	FIFIs about manage key dependencies required to support the EDRP, such as: Information security requirements for data security and storage (e.g., encyption); and, Location of technology asset centres, backup sites, service provider locations and poisimity to primary data centres, and other critical technology assets and locations. Principle 13: FRFIs aboutd perform senario testing on diasater recovery capabilities to contrim its technology services operate as expected	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	
2.9.2	Key dependencies are managed	Discuss fraction. PTPIs should manage key dependencies required to support the EDRP, such as: information security requirements for data security and storage (e.g., encyption); and, Location of technology asset centres, backup aites, service provider locations and portunity to primary data centres, and other critical technology assets and locations. Principle 13: RFIs ahoud perform senario testing on diasater recovery capabilities to confirm fla technology services operate as expected	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Machaniams exist to identify and assess the security of technology assets that support more than one critical business function.	5	
2.9.2	Key dependencies are managed	Part about the container of the container of the container of the CDRP, auch as: Information security requirements for data security and storage (e.g., excyption); and, Location of technology asset centres, backup sites, service provider locations and postmit to primary data centres, and other critical technology assets and locations. Principle 13: FRFM should perform secansito testing on disaster recovery capabilities to confirm its technology services operate as expected thorough disaster.	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	
2.9.2	Key dependencies are managed	Anounth incustion. PPINs should incuston. PPINs should incuston the EDRP, such as: information accurity requirements for data security and storage (e.g., encryption; and, Location of technology asset centres, backup attes, service provider locations and proximity to primary data centres, and other critical technology assets and locations. Principle 13. PPINs should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected thorush desirucha.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should manage key dependencies required to support the EDRP, such as:					Mechanisms exist to protect sensitive/regulated data wherever it is stored.	(optional)	
2.9.2	Key dependencies are managed	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.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2		5	
		Principle 13: FRFIs should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected through discution							
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, Locations and proximity to primary data centres, and other critical technology assets and locations.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisme exist to inventory, document and maintain data flows for data that is readent (permanently or temporarily within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or ahared with other third-parties.	5	
		Principle 13: FRFIs should perform scenario testing on disaster recovery cspabilities to confirm its technology services operate as expected through discussion							
		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:					Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.		
2.9.3	Disaster recovery scenarios are tested	New and emerging risks or threads; Material changes to business objectives or technologies. Struations that can lead to protorged outage; and, Previous incident history and known technology complexities or weakness. FRFIs' disaster recovery scenarios should test:	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04		5	
		The FRF* is backup and recovery capabilities and processes to validate realiency 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 of-premises Outcome: A secure technology posture that maintains the			Cybersecurity & Data		Mechaniama exist to facilitate the implementation of cybersecurity & data protection		
3	Cyber security	confidentiality, integrity and availability of FRFIs' technology assets.	Functional	Subset Of	Protection Governance Program	GOV-01	governance controls. Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
3	Cyber security	confidentiality, integrity and availability of FRFIs' technology assets.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
3	Cyber security	Outcome: A secure technology posture that maintains the confidentiality, integrity and availability of FRFIs' technology assets.	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
3	Cyber security	Outcome: A secure technology posture that maintains the confidentiality, integrity and availability of FRFIs' technology assets.	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, resoonse and recovery activities.	10	
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	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	
3.0	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	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	
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	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	
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	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	
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	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	
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 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	
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	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	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	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	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	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. FRFIs should identify current or emerging cyber threats proactively using	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisme exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
3.1.1	Security risks are identified	FRFs should identify current or emerging cyber threats proactively using threat assessments to evaluate threats and assess security tits. 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 Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	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 Catalog	RSK-03.1	Mechanisms exist to device and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	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 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	
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 Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	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	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	
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	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker factor, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	

version 2025.2	
6/26/2025	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
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	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.	(optional) 5	
3.1.2	Intelligence-led threat assessment and testing is conducted	assessments, processes, and tools to cover controls at different layers defence. FRFIs should adopt a risk-based approach to threat assessment and testing. FRFIs should also the different layers, and minihum the quencies, for intelligence-led theat assessments to test oper accurity processes and controls. FRFIs should also regularly perform tests and exercises, to identify vulnerabilities or control spin in its oper ascurity programs (e.e., perturbation testing and red teaming) using an intelligence-led approach. The score and potential imputs of such testing bloud bb clearly defined by the FRFI with effective risk mitigation controls applied troughout the assessment to manage any associated internet risks.	Functional	Equat	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	
3.1.2	Intelligence-led threat assessment and teating is conducted	FRFs should adopt a risk-based approach to threat assessment and testing. FRFs should set deflect triggers, and minimum frequencies, for utilitigation-tel diffue that assessments to set of yoler acourty processes and controls. FRFs should also regularly perform tests and exercises, to identify vulnerabilities or control gaps in its cycler socurity roggems (e.g. perturbation testing and red teaming) using an intelligence-ted approach. The socie and potential impactor of such testing bload db clearly defined by the FRFI with effective risk mitigation controls applied houghout the assessment to manage or associated internet risks.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	2	
3.1.2	Intelligence-ted threat assessment and testing is conducted	FIFIs should adopt a risk-based approach to threat assessment and testing. FRRs should adopt and end disk disk and the should be adopt and the should	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	FRFs includ establish processes to conduct regular vulnerability assessment of the technology assess, including but not futilited to network devices, systems and applications. Processes should articulate the frequency with which vulnerability cars and assessments are conducted. FRFs should assess and rank relevant other vulnerabilities and threast according to the severity of the threat and risk seponue to technology assets using a standard risk measurement methodology. In ding as, PRFs lavoid consider the potential cumulative impact of vulnerabilities, irrespective of risk (twel, that could present a high-risk seponure when combined.	Functional	Intersects With	Vutnerability Ranking	VPM-03	Mechaniame exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
3.1.3	Vulnerabilities are identified, assessed and ranked	FR1s should establish processes to conduct regular vulnerability assessments of its technology assets, including but not limited to network devices, systems and applications. Processes should arriculate the frequency with which vulnerability scans and assessments are conducted. FR1s hould assess and rark relevant cyber vulnerabilities and threats according to the severity of the threat and risk exposure to technology assets using a standard risk measurement methodogo. In doing so, FR1s should consider the potential cumulative impact of vulnerabilities, irrespective of risk level, that could present a high-risk exposure when combined.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.1.4	Data are identified, classified and protected	FRFIs should ensure that adequate controls are in place to identify, classify and protect structured and unstructured data based on their confidentiality classification. FRFIs bandl implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unsuftorized access.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.1.4	Data are identified, classified and protected	FRFs should ensure that adequate controls are in place to identify, classify and protect structured and unstructured data based on their confidentiality classification. FRFs is hould implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unsufthritized access.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechaniama exist to protect sensitive/regulated data wherever it is stored.	5	
3.1.4	Data are identified, classified and protected	FRFs should ensure that adequate controls are in place to identify, classify and protect structured and unstructured data based on their confidentiality classification. FRFs should implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unsufthritide acress.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisma exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
3.1.4	Data are identified, classified and protected	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 unsufthritide acress.	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	
3.1.4	Data are identified, classified and protected	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 unsultivitized acress.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to liveritory, document and maintain data flows for data that is existent (permanently of temporarily) within a service's grappincially 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	FRFs should maintain continuous situational awareness of the external cyber threat landscape and Is threat environment as It applies to its technology asset. This could include participating in industry threat intelligence and information sharing forums and subscribing to timely and reputable threat information source. Where Results, CFRFs are encouraged to provide timely exchange of threat intelligence to facilitate prevention of cyber attacks, threaby contributing to its own cyber resilience and that of the throady 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 regularity 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	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	
3.1.6	Threat modelling and hunting are conducted	Incluing a financial strain and a second strain and a second strain and second strain strain should be assessed regularly to enhance the opter security program, capabilities and controls required to mitigate current and services, capabilities and controls required to mitigate current and services that threats which may not be detected by automated to do le it meta humania.	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	
3.1.6	Threat modelling and hunting are conducted	Where feasible, FRI's should maintain cyber threat models to dentify ober security threats directly facing its technology assess and services. Thesats should be assessed regularly to enhance the cyber security program, capabilities and controls required to mitigate current and emerging threats. TRI's should use manual techniques to proactively identify and isolate threats which may not be detected by automated threats are introls.	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	
3.1.6	Threat modelling and hunting are conducted	Where feasible, FRI's should maintain cyber threat models to identify opter security threat directly facing its technology assets and envices. Threats should be assessed regularly to enhance the cyber security program, capabilities and controls required to mitigate current and emerging threats. FRI's should use manual techniques to proactively identify and isolate threats which may not be detected by automated facils <i>i.e.</i> threat human.	Functional	Intersects With	Threat Analysis	THR-10	Mechaniams 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	FRFs should enable and encourage its employees, customers and third parties to report suspicious optice archive, recognizing the role that each can play in preventing optior tatacis. FRFs should create awareness of optier attack scenarios directly tagging employees, customers and relevant third parties. In addition, the FRFs should regularly test its employees to assess their awareness of coper threats and the affectiveness of their reporting processes and tools.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechaniama exist to facilitate the implementation of security workforce development and awareness controls.	10	

version		
6/2	6/2025	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should enable and encourage its employees, customers and third	nationale	- netationship			Control Description Mechanisms exist to provide all employees and contractors appropriate awareness	(optional)	
3.1.7	Cyber awareness is promoted and tested	parties to report suspicious cyber activity, recognizing the role that each can play n preventing cyber attacks. FRI's should create awareness of cyber attack scenarios directly targening employees, customers and relevant third parties. In addition, the FRI should regularly test its employees to assess their awareness of cyber threats and the effectiveness of their reporting processes and tools.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	education and training that is relevant for their job function.	5	
3.1.7	Cyber awareness is promoted and tested	FPRs hould enable and encourage its employees, customers and third parties to report suspicious opera existiv, recognizing the one that each can play in greening oper tables. FPRIs should create awareness of oper stack: scenarios directly targeting employees, customers and relevant third parties. In addition, the FRFs should regularly test its employees to assess that awareness of cyber threats and the effectiveness of their reporting processes and looks.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurty & data privacy-related training: (1) Berlow authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.1.7	Cyber awareness is promoted and tested	FIFIs bould enable and encourage its amployees, customers and third particle to report supplicitus operator script, recepting the role that each can play in preventing other tables. FIFIs should create aneureness of opera stack scenarios of incertly targeting employees, customers and relevant third parties. In addition, the FIFIs should regularly test its employees to assess their avancess of cyber threats and the effectiveness of their reporting processes and tools.	Functional	Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity & data privacy training that reinforce training objectives.	3	
3.1.7	Cyber awareness is promoted and tested	FIFIs should enable and encourage its amployees, customers and third particle to report surplicitus operate strating, recepting the role that each can play in preventing other tables. FIFIs should create anerteness of oper stratic scenarios directly targeting employees, customers and relevant third patters. In addition, the FFFI should regularly test its employees to assess their aveneses of cyber threats and the effectiveness of their reporting process and tools.	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 are on oseing internal and actematir isk 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) Onter sinds 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	
3.1.8	Cyber risk profile is monitored and reported on	FIPEs should maintain, and report on, a current and comprehensive ober security risk profiles for bolitates everigit and timely decision- making. The profile should draw on existing internal and external risk identification and assessment sources, processes, tools and capabilities. FIPEs should also ensure that processes and tools exist to measure, monitor and aggregate residual risks.	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
3.1.8	Cyber risk profile is monitored and reported on	FPFs bould maintain, and report on, a current and comprehensive cyber security risk profis to facilitate oversight and timely decision- maing. The profits bould arw on existing internal and external risk identification and assessment sources, processes, tools and capabilities. FPFs should also ensure that processes and tools exist to measure, monitor and aggregate residual risks.	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	
3.1.8	Cyber risk profile is monitored and reported on	FPRs backed 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. FPRs should also ensure that processes and tools exist to measure, monitor and aggregate residual risks.	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	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,	10	
3.2	Defend	technology assets. Principle 15: FRFIs should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	implementation and modification of systems and services. 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 tessible, and FRFIs abuild 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	
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 gain to be preventive, where establish, and FRFIs abuild 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	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cyberescurity & data privacy practices for each system, application and/or service under their control.	5	
3.2.1	Secure-by-design practices are adopted	FIFIs should adopt secure by design practices to safeguard its technology assets. Security defence controls should am to be preventive, where feasible, and FIFIs should regizinfar verview security use cases with a view to strengther reliance on preventive writes and the security controls should be applied end- form, straining after design stage, to applications, micro-services and application programming interfaces developed by the FRFI.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilities the implementation of industry-recognized optensecurity & data privecy protices in the specification, design, development, implementation and modification of systems and services.	10	
3.2.1	Secure-by-design practices are adopted	FIFIE should adopt secure by design practices to sentgeant its section logic assets. Security defines controls should any the boot seventher, where feasible, and FIFIs should regularly review security use cases with a view to strengthen relince on privantiles writing detective controls. Standard security controls should be applied end- cot, starting at the design stage, to capitalizations, micro-envices and application programming interfaces developed by the FRFI.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Machaniams exist to achieve resilience requirements in normal and adverse situations.	3	
3.2.2	Strong and secure cryptographic technologies are employed	FRFs should implement and maintain strong cryptographic technologies to protect the suthenticity, confidentiality and integrity of its technology sease. This includes controls for the protection of encryptom keys for unsuthorised access, usage and disclosure throughout the cryptographic key management (Ite cyclic. FRFs should regularly assess la cryptography standard and technologies to remain effective against current and emerging threats.	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	
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 stats. This includes controls for the protection of encryptic tables have the unautographic bary may appear and the content of the protection of encryptic party induced and technologies to remain effective against current and emerging threats.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechaniams exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
32.3	Enhanced controls and functionality are applied to protect critical and external- facing technology assets	FPRs hould employ enhanced controls and functionality to rapidly contain cyber security threats, diefed is circital technology assets and remain realient against cyber attacks by considering the following: lidentifying 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 handening requirements, and Deploying additional tayers 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	Mechanisma exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	

version 2025.2	
6/26/2025	
0/20/2023	

FDE #	FDE Name	Focsl Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRPs should implement and maintain multiple layers of cyber security controls and defend against cyber security threats at every stage of the taback life cycle (e.g. from reconsistance and initial access to securiting on objectives). FRPIs should also ensure realisince against current and emerging cyber threats by nimitaining defence controls and tools. This includes ensuring continuous operational effectiveness controls by miniming failse positive. Where feasible, FRPIs should:					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.	(optional)	
324	Cyber security controls are tayered	Protect networks, including external-facing services, from threats by minimizing its attack surface: Define subtroated logical networks cares and apply controls to segregate and limit, or block access and traffic to and from network zones: Leverage a combination of allow/define statistics, nackang fite integrity checks (e.g., fite hash heighting) and indicators of compones, in a continuously policities and an advection capabilities that are continuously policities, and apply defines controls and capabilities for intrusion prevention and detection on its network perimeter in addition to controls for data loss, mahware and viruses.	Functional	Intersects With	Layered Network Defenses	NET-02		5	
324	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 should implement against cyber security threats at every stage of the security of the cyber security threats and the cyber security and the cyber security of the security security and security of the security cyber security and the security and security of the security cyber security security and controls by minimizing fastic positives. Where feasible, FRFIs a hould: Protect networks, including coetranist-facing services, from threads by minimizing fastic security controls to segregate and think, or block coetes and rapidy controls to segregate and think. Disclose coets and fastic coets and from network cores; Leverage a combination of allow/deny tists, including file integrity checke (se.g., file harking same) and indicators of compromise, in addition to advanced behaviour-based protection capabilities that are continuously updated; and Apply defence controls and capabilities for intrusion prevention and detection on its network permitter in addition to controls for data loss, mahaves and viruses.	Functional	Subset Of	Defonse-in-Depth (DD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing impractions 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, FRIs 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	
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	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	
32.6	Security vulnerabilities are remediated	To ensure security vulnerabilities are well managed, FRFIs should: Maintain capabilities to ensure timely risk-based patching of vulnerabilities, in workor software and internal applications, that consides the severity of the threat and vulnerability of the exposed systems; Apply patches at the earliest opportunity, commensurate with risk and in accordance with the ataliest opportunity, commensurate with risk and inscordance with estabilished timelines; Implement compensating controls as needed to sufficiently mitigate insk when emediation options are not available (e.g., "zero-day" attacks), and Regularly monitor and report on patching status and vulnerability remediation against defined timelines, including any backtog and executions	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisma exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
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, invendor software and internal applications, that considers the severity of the threat and vulnerability of the exposed systems: Apply patches at the earliest apportunity, commensurate with risk and in accordance with the abilitiest timelines; risks when remediation options are not available (e.g., "zero.dsy" attacka); and report on patching status and vulnerability Regularly monitor and report on patching status and vulnerability remediation against defined timelines.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisma exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
326	Security vulnerabilities are remediated	To ensure security vulnerabilities are well managed, FRFIs should: Maintain capabilities to ensure timely risk-based patching of vulnerabilities, investor 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 accordance with estabilished trainies; Implement compensating controls as needed to sufficiently mitigate itsk when remediation options are not available (e.g., "zero-day" attacks) and Regulary monitor and report on patching status and vulnerability remediation against defined timelines, including any backtog and	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
327	Identify and access management controls are implemented	FRFB should implement risk based identity and access controls, including Multi-Factor Automicistical of MPA and privileged access management. Where feasible, FRFB should consider: Enforcing the principles of least privilege, conducting regular attestation docess and maintaining strong complex passwords to subtenticate employee, customer and Thirlp-anty access to technology assets; implementing MPA access external-france channels and privileged accounts (e.g. customers, employees, and third parties); Managing privileged account activity as part of continuous security Logging and monitoring accounts activity as part of continuous security managed and monitoring account activity as part of continuous security ensuing appropriate baciground checks (where feasible) on persons partial access to the PFP's systems or data, commensature with the criticality and classification of the technology assets.	Functional	Intersects With	identity & Access Management (IAM)	IAC-01	Mechanisma exist to facilitate the implementation of identification and access management controls.	5	
32.7	Identify and access management controls are implemented	PRFIs should implement risk-based identity and access controls, including Multi-Retor Authentication OFM 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 submericity employee, castomeria of third particles passwords to submericity implementing MFA access external-facing channels and privileged accounts (e.g. cuotienter, employee, and third particle); Managing privileged account redentitals using a secure wait: monitoring: Ensuing system and service accounts are securely submitticated, managed and monitored to detect unsubmittice usage; and Performing appropriate background check (where feasible on persons granted access to the FRFI's systems or data, commensurate with the critically and classification of the technology assets.	Functional	Intersects With	Mutti-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote newex access: (2) Thirdy 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	

FDE #	FDE Name	Focst Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should implement risk-based identity and access controls, including Multi-Factor Authentication (MFA) and privileged access					Mechanisms exist to restrict and control privileged access rights for users and services.	(optional)	
3.2.7	Identify and access management controls are implemented	management. Where feasible, FRFIs should consider: Enforcing the principles of teast privilega, conducting regular attestation of access and maintaining strong complexe passwords to subheriticate employee, customer and third-party access to technology assets; implementing HRF access external-facing channels and privilegad accounts (e.g., customers, employees, and third parties); Managing privilegad account redefinities using a secure wult; Logging and monitoring account activity as part of continuous security monitoring; Ensuring approgram desired accounts are accurely suthenticated, managed and monitored to detect unarbitrized usage; and Performing apprograms background checks (where feasibile) on persons granted access to the FRFI's systems or data, commensurate with the cricicality and classification of the technology assets.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16		5	
32.7	Identity and access management controls are implemented	FRFIs should implement risk-based identity and access controls, including Multi-Ractor Authentication (MFA) and privileged access management. Where Reading, FRFI solutio consider: Enforcing the principles of least privilege, conducting regular attestation of access and maintaining strong complex passwords to sufferent account (e.g., countoners, employees, and third parties); Manging privileged account credentition suring a sector wait; Logging and monitoring account activity as part of continuous security monitoring appropriate background horized and surger subtractated, managed and monitored to detect unactiviticated and performing appropriate background checks (where feasible) on persons granted access to the FRF1's system or data, commensurate with the criticatily and classification of the technology assets.	Functional	Intersects With	Least Privilege	IAG-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
3.2.7	Identity and access management controls are implemented	PRFIs should implement tak-based identity and access controls, including Multi-Pacor Authentication (MFA) and privileged access management. When Beablish, FRFIs should consider: Enforcing the principles of tasks privilege, conducting regular attestistion depolyses, outsioner and third-party access to technology assets; they access and maintaining strong concept channels and privileged accounts of another access the strong channels and privileged accounts of a score acternal regin channels and privileged accounts (e.g. customers, employees, and third parties); Manging privileged account credentities using a secure wult; Logging and monitoring account activity as part of continuous security monitoring: Ensuring appropriate background checks (where feasible) on persons grand access the FRF's system or data, commensurate with the criticality and classification of the technology assets;	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: (2) When the event cocurred; (2) When the event cocurred; (3) When the event cocurred; (4) The outcome of the event: (5) The outcome of the event: (6) The identify 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 inchnology asets and security derence tools, including those provided by third parties. Where possible, ascurity 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	
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	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	
3.2.8	Security configuration baselines are enforced and deviations are managed		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	
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 and the statement of the st	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	
3.2.9		Where feasible, static and/or dynamic acanning and testing capabilities should be used to nearine new, and/or changes to existing systems and applications are assessed for vulnerabilities prior to release into the production environment. Security control as should also be implemented to maintain accurity when development and operations practices are combined through a continuous and automated development pipeline (see paragraph 2.42).	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisma 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	
3.2.9		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 areassed for vulneabilities 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	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	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.2.10	Physical access controls and processes are applied	hazards. FRFs 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	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	
3.3	Detect	Principle 16: FRFIs design, implement and maintain continuous security detection capabilities to enable monitoring, alerting and forensic investigations.	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	
3.3	Detect	Principle 16: FRFIs design, implement and maintain continuous security detection capabilities to enable monitoring, sterting and forensic investigations.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation 2) Automated event detection or manual incident report intake; (2) Analysis; (4) Containment; (5) Eradication; and IN Bacyonery	5	
3.3.1	Continuous, centralized security logging to support investigations	FIFIs should ensure continuous security logging for technology asste and afferent layers of denote tools. Central tools for agragming, correlating and managing security event logs should enable timely log access during scyler event investigation. For any significant cyber threat or incident, the FRP's formatic investigation should not be limited or indigenet and timely and the original constraints of the security event logs. FRP's should implement minimum security log retention periods and maintain cybes evenuty 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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		FRFIs should ensure continuous security logging for technology assets	nationate	ricationship			Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar	(optional)	
3.3.1		and different layers of defence tools. Central tools for aggregating, correlating and managing security event (logs should enable inney) tog access during a cyber event investigation. For any significant cyber threat or incident, the FRF1's forensic investigation should not be limited or delayed by disaggregated, inaccessible or missing critical security event logs. FRF1s should implement minimum security log retention periods and ministina (cyber acuity event) gas to failable a thoorgh and unimpeded forensic investigation of cyber security events.	Functional	Intersects With	Automsted Tools for Real- Time Analysis	MON-01.2	automated tool, to support near real-time analysis and incident escalation.	5	
3.3.1	Continuous, centralized security logging to support investigations	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	Intersects With	Security Event Monitoring	MON-01.8	Mechaniams exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.3.1	Continuous, centralized security logging to support investigations	FRFB should ensure continuous security logging for technology assets and different tayes of defence tools. Central tools for aggraghing, correlating and managing security event logs should enable timely tog access during expere vent investigation. For any significant cycler threat or incident, the FRFP's forensit investigation should not be limited or delayed by diaggrapped, inaccessible to missing critical security event logs. FRFs should imglement minimum security tog retention periods and ministria cycles excurity event togs to focultation a through and unimpeded forensic investigation of cyber security events.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisma exist to utilize a Security incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event loga.	5	
3.3.1	Continuous, centralized security logging to support investigations	FPFIs bloud ensure continuous security logging for tuchnology asets and different layers of defance tools. Cantenit loads for aggregating, correlating and managing accurity event logs should enable timely log access during a cytere weret investigation in boot do not be limited or delayed by disaggregated, inaccessible or missing critical accurity event logs. PFFIs should implement minimum security log retention periods and maintain cytes eurity event period tool tool tool tool and and unimpeded forensic investigation of cyter security events.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from cross the enterprised by a Security Incident Event Manages (SEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
3.3.1		FRFIs should ensure continuous security logging for technology assets and afferent layers of defence tools. Central tools for aggraphing, correlating and managing security event logs should enable timely tog access during a opter event investigation. For any significant cycler threat or incident, the FRFI's forensic investigation should not be limited or delayed by diaggraphed, inaccessible to missing critical security event logs. FRFIs should implement minimum security tog retention periods and maintain cycles everity event logs to focilitate a through and unimpeded forensic investigation of cyber security events.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
3.3.1		FPFs should ensure continuous security logging for technology assets and different ispen of defance tools. Cancello tools for aggraphing, correlating and managing security event logs should enable timely log access during a cytere vent investigation should not be limited or or incident, the FRFs's formalic investigation should not be limited or degles tips should implement minimum security log retention periods and maintain cytes everity event glass tools toolicitate a throopain and unimpeded forensic investigation of cyber security events.	Functional	Intersects With	System-Wide / Time- Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trait that is time-correlated.	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. Cental tools for aggraphing, correlating and managing security event logs should enable timely tog access during a cytere went investigation. For any significant cyter threat or incident, the FRFI's formalic investigation should not be limited or delayed by diaggraphid, inaccessible or missing critical security event logs. FRFIs should implement minimum security tog retention periods	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisme exist to configure systems to produce event logs that contain sufficient information, to a ten inimium: (1) Estabilish what type of event occurred; (2) When (date and time) the event occurred; (3) When the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; (6) The outcome (success or failure) of the event; (7) The ou	5	
3.3.2	Maticious and unauthorized activity is detected	FRFs should maintain security information and event management capabilities to ensure continuous detection and setting of malicious and unauthorized user and system activity. Where feasible, advanced behaviour-based detections and grevenion methods should be used to detect user and entity behaviour anomalies, and emerging external and ismenal threats. The latest threat intellingers and indicators of compromise should be used to continuously enhance FRFI monitoring	Functional	Subset Of	Continuous Monitoring	MON-01	Mechaniama exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.2	Malicious and unauthorized activity is detected	To RFT a should maintain security information and event management capabilities to event continuou detection and advertige of malicious and unauthorized user and system actively. Where feasible, advanced behaviour-based detections and prevention methods should be used to detect user and entity behaviour anomalies, and emerging external and unemail threats. The least threat intelligence and indicators of compromise should be used to continuously enhance FRFI monitoring trade.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechaniame exist to implement intrusion Detection / Prevention Systems (IDS // PS) technologies on critical systems, key network segments and network choke points.	5	
3.3.2	Malicious and unauthorized activity is detected	FPFIs broad maintain security information and event management capabilities to ensure continuous detection and alerting of malicious and unastitutized user and system actively. Where feasible, advanced behaviour-based detection and prevention methods should be used to detect user and entity behaviour anomalies, and emerging external and immant threats. The latest threat integlicence and indication of compromise should be used to continuously enhance FRFI monitoring trues.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms axist to centrally collect, review and analyze audit records from multiple sources.	5	
3.3.2	Malicious and unauthorized activity is detected	FPEIs biolard maintain security information and event management capabilities to enviro continuous detection and alerting of malicious and unastitutized user and system actively. Where feasible, advanced bahvaour-based telections and grevenion methods should be used to detect user and entity behaviour anomalies, and emerging external and internal threats. The least threat intelligence and indication of compromise should be used to continuously enhance FRFI monitoring tools.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (poC).	5	
3.3.2	Malicious and unauthorized activity is detected	and the should maintain security information and event management capabilities to event continuous detection and setting for malicious and unantibulized user and system activity. When feasible, advanced behaviour-based detection and greenom nontholds should be used to detect user and entity behaviour anomalies, and emerging setternal and isternal threats. The latest threat initiative and indicators of compromise should be used to continuously enhance. FFR monitoring non-	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomatous behavior that could indicate account compromise or other malicious activities.	5	
3.3.3	Cyber security alerts are triaged		Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event ditection or manual incident report intake; (2) Analysis; (4) Containment; (5) Endication; and Becnever	10	
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	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	operational disruption. Principle 17: FRFIs should respond to, contain, recover and learn from cyber security incidents impacting their technology assets, including	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	10	
3.4.1	Incident response capabilities are integrated and aligned	Incidents ordinatine at this dearty oroxidem. Domain 2 sets out the foundational expectitions for FRFs' incident and problem management capabilities. FRFs should ensure the alignment and innegration between their cyber accurity, technology, crisia management and communication protocols. This should include capabilities to enable comprehensive and timely ascalation and stakeholder coordination (internal and external) in response to a major <i>inder security ream of insistent</i> .	Functional	Subset Of	Incident Response Operations	IRO-01	Incidents. Mechanisma exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy- related incidents.	10	
3.4.1	Incident response capabilities are integrated and aligned	Domain 2 sets out the foundational expectations for FRPs' incident and problem management capabilities. FFR's houd ensure the alignment and integration between their oyber security, technology, crisis management and communication protocols. This should include capabilities to enable comprehensive and timely escalation and stakenolder coordination (internal and external) in response to a major cyber security event or incident.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisme seist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (4) Containment; (6) Endication; and (8) Recoverv.	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 (optionsi)
3.4.1	Incident response capabilities are integrated and aligned	Domin 2 sets out the foundational expectations for FRFs incident and problem management capabilities. FRFs should ensure the alignment and integration between their opker accurity, technology, crisis management and communication protocols. This should include capabilities to enable comprehensive and timely secalation and stakeholder coordination (internal and external) in response to a major other servitive ware in clinicities.	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	
3.4.1	Incident response capabilities are integrated and aligned	Domain 2 sets out the foundational expectations for FRFB' incident and problem management capabilities. FRFB's should ensure the alignment and integration between their oyber excurity, technology, crisis management and communication protocols. This should include capabilities to enable comprehensive and intensy secalation and stakeholder coordination (internal and external) in response to a major notes exeruity wave to incident	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisme exist to timely-report incidents to applicable: (1) Internet stateholders; (2) Affected clients & third-parties; and (2) 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	Mechanisma exist to identity 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	FRFs 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; (2) Analysis; (4) Containment; (5) Endication; and B Rennerv.	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	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	FPFBs should establish a cyber incident response steam 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 FRFP'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; (2) Analysis; (4) Containment; (5) Endication; and III Berower	10	
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 stateholdres.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity. If 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	FPIPs bould conduct to forensic investigation for incidents where technology assets may have been materially exposed. For high-severity incidents, the FPI baudd conduct a detailed post-incident assessment of direct and indirect impacts (financial and/or non-financial), including a roct cause analysis to identify remediation actions, address the roct cause and respond to lessons learned. The root cause analysis should assess threats, weaknesses and vulnerabilities in its people, processes, technology and data.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensica and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
3.4.5	Forensic investigations and root cause analysis are conducted, as necessary	FPFB should conduct is forensic investigation for incidents where technology assets may have been materially exposed. For high-severity indicates, the FPB should conduct a detailed post-incident assessment of direct and indirect impacts (financial and/or non-financial), including a roct cause analysis to identify remediation actions, address the root cause and respond to lessons learned. The root cause analysis should assess threats, vexienses and vulnerabilities in its people, processes, technology and data.	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	

17 of 17