NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Preface	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2	Application of the MAS Technology Risk Management Guidelines	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3	Technology Risk Governance and Oversight	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.1	Role of the Board of Directors and Senior Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.1.1	Role of the Board of Directors and Senior Management	Technology is a key business enabler in the financial sector and FIs rely on technology to deliver financial services. It is vital that the FI's board of directors and senior management ensure effective internal controls and risk management practices are implemented to achieve security, reliability and resilience of its IT operating environment.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.2	Role of the Board of Directors and Senior Management	Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which include risks posed by cyber threats.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.3	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure a Chief Information Officer, Chief Technology Officer or Head of IT, and a Chief Information Security Officer or Head of Information Security 1 , with the requisite expertise and experience, are appointed. The appointments should be minimally approved by the Chief Executive Officer.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
3.1.3	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure a Chief Information Officer, Chief Technology Officer or Head of IT, and a Chief Information Security Officer or Head of Information Security 1 , with the requisite expertise and experience, are appointed. The appointments should be minimally approved by the Chief Executive Officer.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.1.4	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure a technology risk management strategy is established and implemented.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
3.1.4	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure a technology risk management strategy is established and implemented.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	8	
3.1.5	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure key IT decisions are made in accordance with the FI's risk appetite.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
3.1.5	Role of the Board of Directors and Senior Management	The board of directors and senior management should ensure key IT decisions are made in accordance with the FI's risk appetite.	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.	8	
3.1.6	Role of the Board of Directors and Senior Management	Given that technology underpins many of the operations and services offered by an FI, the board of directors and senior management should set the tone from the top and cultivate a strong culture of technology risk awareness and management at all levels of staff within the FI.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	8	
3.1.6	Role of the Board of Directors and Senior Management	Given that technology underpins many of the operations and services offered by an FI, the board of directors and senior management should set the tone from the top and cultivate a strong culture of technology risk awareness and management at all levels of staff within the FI.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	8	
3.1.7	Role of the Board of Directors and Senior Management	The board of directors or a committee delegated by it, is responsible for:	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(a)	Role of the Board of Directors and Senior Management	ensuring a sound and robust risk management framework is established and maintained to manage technology risks;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(a)	Role of the Board of Directors and Senior Management	ensuring a sound and robust risk management framework is established and maintained to manage technology risks;	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	
3.1.7(b)	Role of the Board of Directors and Senior Management	ensuring there is a technology risk management function to oversee the technology risk management framework and strategy, as well as to provide an independent view of the technology risks faced by the FI;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(c)	Role of the Board of Directors and Senior Management	giving senior executives, who are responsible for executing the FI's technology risk management strategy, sufficient authority, resources and access to the board of directors;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(c)	Role of the Board of Directors and Senior Management	giving senior executives, who are responsible for executing the FI's technology risk management strategy, sufficient authority, resources and access to the board of directors;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3	
3.1.7(c)	Role of the Board of Directors and Senior Management	giving senior executives, who are responsible for executing the FI's technology risk management strategy, sufficient authority, resources and access to the board of directors;	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3	
3.1.7(d)	Role of the Board of Directors and Senior Management	approving the risk appetite and risk tolerance statement that articulates the nature and extent of technology risks that the FI is willing and able to assume;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(d)	Role of the Board of Directors and Senior Management	approving the risk appetite and risk tolerance statement that articulates the nature and extent of technology risks that the FI is willing and able to assume;	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
3.1.7(d)	Role of the Board of Directors and Senior Management	approving the risk appetite and risk tolerance statement that articulates the nature and extent of technology risks that the FI is willing and able to assume;	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	
3.1.7(e)	Role of the Board of Directors and Senior Management	undertaking regular reviews of the technology risk management strategy for continued relevance;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(f)	Role of the Board of Directors and Senior Management	assessing management competencies for managing technology risks; and	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.7(g)	Role of the Board of Directors and Senior Management	ensuring an independent audit function is established to assess the effectiveness of controls, risk management and governance of the FI.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
3.1.8	Role of the Board of Directors and Senior Management	Senior management is responsible for:	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.1.8	Role of the Board of Directors and Senior Management	Senior management is responsible for:	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.1.8(a)	Role of the Board of Directors and Senior Management	establishing the technology risk management framework and strategy;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.1.8(b)	Role of the Board of Directors and Senior Management	managing technology risks based on the established framework and strategy;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.1.8(c)	Role of the Board of Directors and Senior Management	ensuring sound and prudent policies, standards and procedures for managing technology risks are established and maintained, and that standards and procedures are implemented effectively;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
3.1.8(c)	Role of the Board of Directors and Senior Management	ensuring sound and prudent policies, standards and procedures for managing technology risks are established and maintained, and that standards and procedures are implemented effectively;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.1.8(d)	Role of the Board of Directors and Senior Management	ensuring the roles and responsibilities2 of staff in managing technology risks are delineated clearly; and	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.1.8(e)	Role of the Board of Directors and Senior Management	apprising the board of directors of salient and adverse technology risk developments and incidents that are likely to have a major impact on the FI in a timely manner.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
3.1.8(e)	Role of the Board of Directors and Senior Management	apprising the board of directors of salient and adverse technology risk developments and incidents that are likely to have a major impact on the FI in a timely manner.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
3.2	Policies, Standards and Procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.2.1	Policies, Standards and Procedures	The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets3 in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
3.2.1	Policies, Standards and Procedures	The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets3 in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
3.2.2	Policies, Standards and Procedures	The FI should ensure risks associated with deviations are thoroughly reviewed and assessed. The risk assessment should be approved by senior management. Approved deviations should be reviewed periodically to ensure the residual risks remain at an acceptable level.	Functional	Subset Of	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	10	
3.2.2	Policies, Standards and Procedures	The FI should ensure risks associated with deviations are thoroughly reviewed and assessed. The risk assessment should be approved by senior management. Approved deviations should be reviewed periodically to ensure the residual risks remain at an acceptable level.	Functional	Intersects With	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	3	
3.2.3	Policies, Standards and Procedures	Compliance processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes for non-compliance.	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
3.3	Management of Information Assets	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.1	Management of Information Assets	To have an accurate and complete view of its IT operating environment, the FI should establish information asset management practices that include the following:	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	
3.3.1(a)	Management of Information Assets	identification of information assets that support the FI's business and delivery of financial services;	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
3.3.1(a)	Management of Information Assets	identification of information assets that support the FI's business and delivery of financial services;	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
3.3.1(a)	Management of Information Assets	identification of information assets that support the FI's business and delivery of financial services;	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
3.3.1(b)	Management of Information Assets	classification of an information asset based on its security classification or criticality;	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
3.3.1(c)	Management of Information Assets	ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
3.3.1(d)	Management of Information Assets	establishment of policies, standards and procedures to manage information assets according to their security classification or criticality.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
3.3.2	Management of Information Assets	The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
3.4	Management of Third Party Services	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.4.1	Management of Third Party Services	The use of certain third party services by FIs may not always constitute outsourcing. However, as many of these services are provisioned or delivered using IT, or may involve confidential or sensitive customer information being stored or processed electronically by the third party, the FI's operations and its customers may be adversely impacted if there is a system failure or security breach at the third party.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
3.4.2	Management of Third Party Services	The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
3.4.2	Management of Third Party Services	The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
3.4.2	Management of Third Party Services	The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.4.3	Management of Third Party Services	On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality4 and integrity as well as ensuring system resilience.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	
3.4.3	Management of Third Party Services	On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality4 and integrity as well as ensuring system resilience.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
3.4.3	Management of Third Party Services	On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality4 and integrity as well as ensuring system resilience.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
3.5	Competency and Background Review	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.5.1	Competency and Background Review	As the human element plays an important role in managing IT systems and processes in an IT environment, the FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
3.5.1	Competency and Background Review	As the human element plays an important role in managing IT systems and processes in an IT environment, the FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
3.5.1	Competency and Background Review	As the human element plays an important role in managing IT systems and processes in an IT environment, the FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.5.1	Competency and Background Review	As the human element plays an important role in managing IT systems and processes in an IT environment, the FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
3.5.2	Competency and Background Review	Insider threat, which includes theft of confidential data, sabotage of IT systems and fraud by staff, contractors and service providers, is considered one of the risks to an organisation. A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimise this risk.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
3.5.2	Competency and Background Review	Insider threat, which includes theft of confidential data, sabotage of IT systems and fraud by staff, contractors and service providers, is considered one of the risks to an organisation. A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimise this risk.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
3.6	Security Awareness and Training	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.6.1	Security Awareness and Training	A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI. The content of the training programme should minimally include information on the prevailing cyber threat landscape and its implications, the FI's IT security policies and standards, as well as an individual's responsibility to safeguard information assets. All personnel in the FI should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
3.6.1	Security Awareness and Training	A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI. The content of the training programme should minimally include information on the prevailing cyber threat landscape and its implications, the FI's IT security policies and standards, as well as an individual's responsibility to safeguard information assets. All personnel in the FI should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
3.6.1	Security Awareness and Training	A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI. The content of the training programme should minimally include information on the prevailing cyber threat landscape and its implications, the FI's IT security policies and standards, as well as an individual's responsibility to safeguard information assets. All personnel in the FI should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5	
3.6.2	Security Awareness and Training	The training programme should be conducted at least annually for all staff, contractors and service providers who have access to the FI's information assets.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.6.3	Security Awareness and Training	The board of directors should undergo training to raise their awareness on risks associated with the use of technology and enhance their understanding of technology risk management practices.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.6.4	Security Awareness and Training	The training programme should be reviewed periodically to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, prevalent and emerging risks, and the evolving cyber threat landscape.	Functional	Subset Of	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	10	
4	Technology Risk Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.1	Risk Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.1.1	Risk Management Framework	The FI should establish a risk management framework to manage technology risks. Appropriate governance structures and processes should be established, with welldefined roles, responsibilities, and clear reporting lines across the various organisational functions.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
4.1.2	Risk Management Framework	Effective risk management practices and internal controls should be instituted to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	8	
4.1.2	Risk Management Framework	Effective risk management practices and internal controls should be instituted to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
4.1.3	Risk Management Framework	The risk owner, who is accountable for ensuring proper risk treatment measures are implemented and enforced for a specific technology risk, should be identified. The role of the risk owner may be assumed by a function or group of functions within the FI, who is given the authority to manage technology risks.	Functional	Intersects With	Risk Owner	RSK-03.2	Mechanisms exist to identify a risk owner for each item in the risk register to ensure clear accountability for unremediated risks.	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.1.3	Risk Management Framework	The risk owner, who is accountable for ensuring proper risk treatment measures are implemented and enforced for a specific technology risk, should be identified. The role of the risk owner may be assumed by a function or group of functions within the FI, who is given the authority to manage technology risks.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance, service provider, etc.); or (4) Accepting the risk.	8	
4.1.4	Risk Management Framework	The framework should also encompass the following components:	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
4.1.4(a)	Risk Management Framework	risk identification – identify threats and vulnerabilities to the FI and information assets;	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
4.1.4(b)	Risk Management Framework	risk assessment – assess the potential impact and likelihood of threats and vulnerabilities to the FI and information assets;	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.1.4(c)	Risk Management Framework	risk treatment – implement processes and controls to manage technology risks posed to the FI and protect the confidentiality, integrity and availability of information assets; and	Functional	Subset Of	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	10	
4.1.4(c)	Risk Management Framework	risk treatment – implement processes and controls to manage technology risks posed to the FI and protect the confidentiality, integrity and availability of information assets; and	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance, service provider, etc.); or (4) Accepting the risk.	8	
4.1.4(d)	Risk Management Framework	risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions; and report key risks to the board of directors and senior management.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	
4.1.4(d)	Risk Management Framework	risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions; and report key risks to the board of directors and senior management.	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	3	
4.1.4(d)	Risk Management Framework	risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions; and report key risks to the board of directors and senior management.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	3	
4.1.5	Risk Management Framework	As business and IT environments, as well as the cyber threat landscape, tend to evolve over time, the FI should review the adequacy and effectiveness of its risk management framework regularly.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
4.2	Risk Identification	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.2.1	Risk Identification	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
4.2.1	Risk Identification	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
4.2.1	Risk Identification	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
4.2.1	Risk Identification	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
4.2.1	Risk Identification	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	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	
4.3	Risk Assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.3.1	Risk Assessment	The FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.3.2	Risk Assessment	To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established.	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.	8	
4.4	Risk Treatment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.4.1	Risk Treatment	The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
4.4.1	Risk Treatment	The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	
4.4.2	Risk Treatment	As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures. The criteria and approving authorities for risk acceptance should be clearly defined and it should be commensurate with the FI's risk tolerance.	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	3	
4.4.2	Risk Treatment	As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures. The criteria and approving authorities for risk acceptance should be clearly defined and it should be commensurate with the FI's risk tolerance.	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.	3	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.4.2	Risk Treatment	As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures. The criteria and approving authorities for risk acceptance should be clearly defined and it should be commensurate with the FI's risk tolerance.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance, service provider, etc.); or (4) Accepting the risk.	5	
4.4.3	Risk Treatment	The FI should take insurance cover for various insurable technology risks to reduce financial impact such as recovery and restitution costs.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance, service provider, etc.); or (4) Accepting the risk.	5	
4.5	Risk Monitoring, Review and Reporting	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.5.1	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
4.5.1	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
4.5.1	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
4.5.1	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
4.5.1	Risk Monitoring, Review and Reporting	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
4.5.2	Risk Monitoring, Review and Reporting	A risk register should be maintained to facilitate the monitoring and reporting of technology risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be commensurate with the level of risk.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
4.5.3	Risk Monitoring, Review and Reporting	To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure. In determining the technology risk metrics, the FI should take into account risk events and audit observations, as well as applicable regulatory requirements.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
5	IT Project Management and Security-by-Design	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.1	Project Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.1.1	Project Management Framework	A project management framework should be established to ensure consistency in project management practices, and delivery of outcomes that meets project objectives and requirements. The framework should cover the policies, standards, procedures, processes and activities to manage projects from initiation to closure.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	8	
5.1.2	Project Management Framework	Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5	
5.1.2	Project Management Framework	Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
5.1.2	Project Management Framework	Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
5.1.3	Project Management Framework	Key documentation in the IT project life cycle, including the feasibility analysis, cost-benefit analysis, business case analysis, project plan, as well as the implementation plan, should be maintained and approved by the relevant business and IT management.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5	
5.1.4	Project Management Framework	As project risks can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
5.1.4	Project Management Framework	As project risks can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle.	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3	
5.2	Project Steering Committee	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.2.1	Project Steering Committee	For large and complex projects that impact the business, a project steering committee consisting of key stakeholders, including business owners and IT, should be formed to provide direction, guidance and oversight to ensure milestones are reached, and deliverables are realised in a timely manner.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
5.2.2	Project Steering Committee	Risks and issues for large and complex projects, which cannot be resolved at the project management level, should be escalated to the project steering committee and senior management.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
5.3	System Acquisition	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.3.1	System Acquisition	The FI should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FI.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
5.3.1	System Acquisition	The FI should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FI.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
5.3.1	System Acquisition	The FI should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FI.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.3.2	System Acquisition	It is important that the FI assesses the robustness of the vendor's software development and quality assurance practices, and ensuresstringent security practices are in place to safeguard and protect any sensitive data the vendor has access to over the course of the project. Any vendor access to the FI's IT systems should be controlled and monitored.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
5.3.2	System Acquisition	It is important that the FI assesses the robustness of the vendor's software development and quality assurance practices, and ensuresstringent security practices are in place to safeguard and protect any sensitive data the vendor has access to over the course of the project. Any vendor access to the FI's IT systems should be controlled and monitored.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
5.3.3	System Acquisition	If a project involves a commercial off-the-shelf (COTS) solution that does not meet the FI's security requirements, the FI should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed.	Functional	Subset Of	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	10	
5.3.4	System Acquisition	The FI should assess if a source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. Suitable alternatives to replace the software should be identified if an escrow agreement could not be implemented.	Functional	Intersects With	Software Escrow	TDA-20.3	Mechanisms exist to escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support.	5	
5.4	System Development Life Cycle and Security-By-Design	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.4.1	System Development Life Cycle and Security-By-Design	The FI should establish a framework to manage its system development life cycle (SDLC). 5 The framework6 should clearly define the processes, procedures and controls in each phase of the life cycle, such as initiation/planning, requirements analysis, design, implementation, testing and acceptance. Standards and procedures for the different phases of the SDLC should be maintained.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
5.4.2	System Development Life Cycle and Security-By-Design	The security-by-design approach refers to building security in every phase of the SDLC in order to minimise system vulnerabilities and reduce the attack surface. The FI should incorporate security specifications in the system design, perform continuous security evaluation, and adhere to security practices throughout the SDLC.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	8	
5.4.3	System Development Life Cycle and Security-By-Design	Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5	
5.4.3	System Development Life Cycle and Security-By-Design	Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
5.4.4	System Development Life Cycle and Security-By-Design	The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
5.5	System Requirements Analysis	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.5.1	System Requirements Analysis	The FI should identify, define and document the functional requirements for the IT system. In addition to functional requirements, key requirements such as system performance, resilience and security controls, should also be established and documented.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5	
5.5.1	System Requirements Analysis	The FI should identify, define and document the functional requirements for the IT system. In addition to functional requirements, key requirements such as system performance, resilience and security controls, should also be established and documented.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
5.5.2	System Requirements Analysis	In establishing the security requirements, the FI should assess the potential threats and risks related to the IT system, and determine the acceptable level of security required to meet its business needs.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
5.5.2	System Requirements Analysis	In establishing the security requirements, the FI should assess the potential threats and risks related to the IT system, and determine the acceptable level of security required to meet its business needs.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
5.5.2	System Requirements Analysis	In establishing the security requirements, the FI should assess the potential threats and risks related to the IT system, and determine the acceptable level of security required to meet its business needs.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
5.6	System Design and Implementation	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.6.1	System Design and Implementation	As part of the design phase, the FI should review the proposed architecture and design of the IT system, including the IT controls to be built into the system, to ensure they meet the defined requirements, before implementation.	Functional	Intersects With	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.	8	
5.6.2	System Design and Implementation	The FI should verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be endorsed by relevant stakeholders.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
5.6.2	System Design and Implementation	The FI should verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be endorsed by relevant stakeholders.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
5.6.2	System Design and Implementation	The FI should verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be endorsed by relevant stakeholders.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.6.3	System Design and Implementation	Relevant domain experts should be engaged to participate in the design review. For example, the security design and architecture of the IT system should be reviewed by IT security specialists or qualified security consultants.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	8	
5.7	System Testing and Acceptance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.7.1	System Testing and Acceptance	A methodology for system testing7 should be established. The scope of testing should cover business logic, system function, security controls and system performance under various load and stress conditions. A test plan should be established and approved before testing.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
5.7.2	System Testing and Acceptance	The FI should trace the requirements during the testing phase, and ensure each requirement is covered by appropriate test cases.	Functional	Intersects With	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.	5	
5.7.3	System Testing and Acceptance	The FI should maintain separate physical or logical environments for unit, system integration and user acceptance testing, and restrict access to each environment on a need-to basis.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
5.7.3	System Testing and Acceptance	The FI should maintain separate physical or logical environments for unit, system integration and user acceptance testing, and restrict access to each environment on a need-to basis.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	5	
5.7.4	System Testing and Acceptance	The FI should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing IT system to validate that it continues to function properly after the changes have been implemented.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5	
5.7.5	System Testing and Acceptance	Issues identified from testing, including system defects or software bugs, should be properly tracked and addressed. Major issues that could have an adverse impact on the FI's operations or delivery of service to customers should be reported to the project steering committee and addressed prior to deployment to the production environment.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
5.7.5	System Testing and Acceptance	Issues identified from testing, including system defects or software bugs, should be properly tracked and addressed. Major issues that could have an adverse impact on the FI's operations or delivery of service to customers should be reported to the project steering committee and addressed prior to deployment to the production environment.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5	
5.7.6	System Testing and Acceptance	The FI should ensure the results of all testing that was conducted are documented in the test report, and signed off by the relevant stakeholders.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	3	
5.7.6	System Testing and Acceptance	The FI should ensure the results of all testing that was conducted are documented in the test report, and signed off by the relevant stakeholders.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
5.8	Quality Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.8.1	Quality Management	During project planning, the FI should define the expected quality attributes and the assessment metrics for the project deliverables based on its quality control standards.	Functional	Intersects With	Quality Management System (QMS)	GOV-18	Mechanisms exist to govern a Quality Management System (QMS) to ensure security, compliance and resilience processes conform with applicable statutory, regulatory and/or contractual obligations.	5	
5.8.1	Quality Management	During project planning, the FI should define the expected quality attributes and the assessment metrics for the project deliverables based on its quality control standards.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
5.8.2	Quality Management	Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI's policies, procedures and standards.	Functional	Subset Of	Quality Management System (QMS)	GOV-18	Mechanisms exist to govern a Quality Management System (QMS) to ensure security, compliance and resilience processes conform with applicable statutory, regulatory and/or contractual obligations.	10	
6	Software Application Development and Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.1	Secure Coding, Source Code Review and Application Security Testing	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.1.1	Secure Coding, Source Code Review and Application Security Testing	Software bugs or vulnerabilities are typically targeted and exploited by threat actors to compromise an IT system, and they often occur because of poor software development practices. To minimise the bugs and vulnerabilities in its software, the FI should adopt standards on secure coding, source code review8 and application security testing.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
6.1.2	Secure Coding, Source Code Review and Application Security Testing	The secure coding and source code review standards should cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
6.1.3	Secure Coding, Source Code Review and Application Security Testing	A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI's software.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
6.1.3	Secure Coding, Source Code Review and Application Security Testing	A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI's software.	Functional	Intersects With	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	5	
6.1.3	Secure Coding, Source Code Review and Application Security Testing	A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI's software.	Functional	Intersects With	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	5	
6.1.4	Secure Coding, Source Code Review and Application Security Testing	To facilitate the remediation of vulnerabilities in a timely manner, the FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI's software.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
6.1.4	Secure Coding, Source Code Review and Application Security Testing	To facilitate the remediation of vulnerabilities in a timely manner, the FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI's software.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	3	
6.1.4	Secure Coding, Source Code Review and Application Security Testing	To facilitate the remediation of vulnerabilities in a timely manner, the FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI's software.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
6.1.5	Secure Coding, Source Code Review and Application Security Testing	The FI should ensure its software developers are trained or have the necessary knowledge and skills to apply the secure coding and application security standards when developing applications.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.1.5	Secure Coding, Source Code Review and Application Security Testing	The FI should ensure its software developers are trained or have the necessary knowledge and skills to apply the secure coding and application security standards when developing applications.	Functional	Intersects With	Continuing Professional Education (CPE) - DevOps Personnel	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	3	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
6.1.6	Secure Coding, Source Code Review and Application Security Testing	It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.	Functional	Intersects With	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	3	
6.1.7	Secure Coding, Source Code Review and Application Security Testing	All issues and software defects discovered from the source code review and application security testing should be tracked. Major issues and software defects should be remediated before production deployment.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
6.1.7	Secure Coding, Source Code Review and Application Security Testing	All issues and software defects discovered from the source code review and application security testing should be tracked. Major issues and software defects should be remediated before production deployment.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5	
6.2	Agile Software Development	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.2.1	Agile Software Development	Agile software development is based on an iterative and incremental development model to accelerate software development and delivery to respond to business and customer needs. When adopting Agile software development methods, the FI should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
6.2.2	Agile Software Development	The FI should ensure secure coding, source code review and application security testing standards are applied during Agile software development.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
6.3	DevSecOps Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.3.1	DevSecOps Management	DevSecOps is the practice of automating and integrating IT operations, quality assurance and security practices in the software development process. It constitutes continuous integration, continuous delivery and IT security practices for frequent, efficient, reliable and secure development, testing and release of software products. The FI should ensure its DevSecOps activities and processes are aligned with its SDLC framework and IT service management processes (e.g. configuration management, change management, software release management).	Functional	Intersects With	DevSecOps	TDA-01.4	Mechanisms exist to integrate security, compliance and resilience into Development, Security and Operations (DevSecOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).	8	
6.3.2	DevSecOps Management	The FI should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8	
6.4	Application Programming Interface Development	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.4.1	Application Programming Interface Development	Application programming interfaces (APIs) 9 enable various software applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIsthat provide developers with programmatic access to a software application or web service. FIs may collaborate with FinTech companies and develop open APIs, which are used by third parties to implement products and services for customers and the marketplace. Hence, it is important for the FI to establish adequate safeguards to manage the development and provisioning of APIs for secure delivery of such services.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
6.4.2	Application Programming Interface Development	A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. The vetting criteria should take into account factors such as the third party's nature of business, cyber security posture, industry reputation and track record.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.4.3	Application Programming Interface Development	The FI should perform a risk assessment before allowing third parties to connect to its IT systems via APIs, and ensure the implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged, and the confidentiality and integrity requirements of the data.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
6.4.4	Application Programming Interface Development	Security standards for designing and developing secure APIs should be established. The standards should include the measures to protect the API keys or access tokens, 10 which are used to authorise access to APIs to exchange confidential data. A reasonable timeframe should be defined and enforced for access token expiry to reduce the risk of unauthorised access.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
6.4.4	Application Programming Interface Development	Security standards for designing and developing secure APIs should be established. The standards should include the measures to protect the API keys or access tokens, 10 which are used to authorise access to APIs to exchange confidential data. A reasonable timeframe should be defined and enforced for access token expiry to reduce the risk of unauthorised access.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
6.4.4	Application Programming Interface Development	Security standards for designing and developing secure APIs should be established. The standards should include the measures to protect the API keys or access tokens, 10 which are used to authorise access to APIs to exchange confidential data. A reasonable timeframe should be defined and enforced for access token expiry to reduce the risk of unauthorised access.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
6.4.5	Application Programming Interface Development	Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
6.4.5	Application Programming Interface Development	Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
6.4.6	Application Programming Interface Development	A robust security screening and testing of the API should be performed between the FI and its third parties before it is deployed into production. The FI should log the access sessions by third parties, such as the identity of the party making the API connections, date and time, as well as the data being accessed.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
6.4.6	Application Programming Interface Development	A robust security screening and testing of the API should be performed between the FI and its third parties before it is deployed into production. The FI should log the access sessions by third parties, such as the identity of the party making the API connections, date and time, as well as the data being accessed.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
6.4.6	Application Programming Interface Development	A robust security screening and testing of the API should be performed between the FI and its third parties before it is deployed into production. The FI should log the access sessions by third parties, such as the identity of the party making the API connections, date and time, as well as the data being accessed.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	8	
6.4.7	Application Programming Interface Development	Detective measures, such as technologies that provide real-time monitoring and alerting, should be instituted to provide visibility of the usage and performance of APIs, and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
6.4.7	Application Programming Interface Development	Detective measures, such as technologies that provide real-time monitoring and alerting, should be instituted to provide visibility of the usage and performance of APIs, and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	8	
6.4.8	Application Programming Interface Development	The FI should ensure adequate system capacity is in place to handle high volumes of API call requests, and implement measures to mitigate cyber threats such as denial of service (DoS) attacks.	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	
6.4.8	Application Programming Interface Development	The FI should ensure adequate system capacity is in place to handle high volumes of API call requests, and implement measures to mitigate cyber threats such as denial of service (DoS) attacks.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
6.5	Management of End User Computing and Applications	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.5.1	Management of End User Computing and Applications	The prevalence of business application tools and software on the Internet has enabled end user computing, where business users develop or use simple applications to automate their operations, such as performing data analysis and generating reports. IT hardware, software and services that are not managed by the IT department (shadow IT) increase the FI's exposure to risks such as leakage of sensitive data or malware infection. Shadow IT should be managed as part of the FI's information assets.	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
6.5.1	Management of End User Computing and Applications	The prevalence of business application tools and software on the Internet has enabled end user computing, where business users develop or use simple applications to automate their operations, such as performing data analysis and generating reports. IT hardware, software and services that are not managed by the IT department (shadow IT) increase the FI's exposure to risks such as leakage of sensitive data or malware infection. Shadow IT should be managed as part of the FI's information assets.	Functional	Intersects With	Shadow Information Technology Detection	OPS-07	Mechanisms exist to detect the presence of unauthorized Technology Assets, Applications and/or Services (TAAS) in use.	5	
6.5.2	Management of End User Computing and Applications	The FI should establish measures to control and monitor the use of shadow IT in its environment.	Functional	Intersects With	Shadow Information Technology Detection	OPS-07	Mechanisms exist to detect the presence of unauthorized Technology Assets, Applications and/or Services (TAAS) in use.	5	
6.5.3	Management of End User Computing and Applications	A process should be established to assess the risk of end user developed or acquired applications to the FI, and ensure appropriate controls and security measures are implemented to address the identified risks, and approval is obtained before being used. The FI should ensure proper testing before the applications are deployed.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
7	IT Service Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.1	IT Service Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.1.1	IT Service Management Framework	A robust IT service management framework is essential for supporting IT services and operations, tracking information assets, managing changes, responding to incidents, as well as ensuring the stability of the production IT environment. The framework should comprise the governance structure, processes and procedures for IT service management activities including configuration management, technology refresh management, patch management, change management, software release management, incident management and problem management.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
7.2	Configuration Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.1	Configuration Management	Configuration management is the process of maintaining key information (e.g. model, version, specifications, etc.) about the configuration of the hardware and software that makes up each IT system. The FI should implement a configuration management process to maintain accurate information of its hardware and software to have visibility and effective control of its IT systems.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.2.2	Configuration Management	The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure it is accurate and up-to-date.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
7.2.2	Configuration Management	The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure it is accurate and up-to-date.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
7.3	Technology Refresh Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.1	Technology Refresh Management	The FI should avoid using outdated and unsupported hardware or software, which could increase its exposure to security and stability risks. The FI should closely monitor the hardware's or software's end-of-support (EOS) dates as service providers would typically cease the provision of patches, including those relating to security vulnerabilities that are found after the EOS date.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	8	
7.3.2	Technology Refresh Management	A technology refresh plan for the replacement of hardware and software should be developed before they reach EOS. A risk assessment for hardware and software approaching EOS date should be conducted to evaluate the risks of their continued use, and effective risk mitigation measures should be implemented.	Functional	Subset Of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	
7.3.3	Technology Refresh Management	The FI should obtain dispensation from its management for the continued use of outdated and unsupported hardware and software. The dispensation should be assigned a validity period that is commensurate with the identified risks and risk mitigation measures. The dispensation should be reviewed periodically to ensure the attendant risks remain at an acceptable level.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
7.3.3	Technology Refresh Management	The FI should obtain dispensation from its management for the continued use of outdated and unsupported hardware and software. The dispensation should be assigned a validity period that is commensurate with the identified risks and risk mitigation measures. The dispensation should be reviewed periodically to ensure the attendant risks remain at an acceptable level.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	8	
7.4	Patch Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.1	Patch Management	A patch management process should be established to ensure applicable functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the FI's IT systems.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
7.4.2	Patch Management	Patches should be tested before they are applied to the FI's IT systems in the production environment to ensure compatibility with existing IT systems or they do not introduce problems to the IT environment.	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-05.6	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	8	
7.5	Change Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.5.1	Change Management	The FI should establish a change management process to ensure changes to information assets are assessed, tested, reviewed and approved before implementation.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
7.5.2	Change Management	A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover factors such as security and implications of the change in relation to other information assets.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
7.5.2	Change Management	A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover factors such as security and implications of the change in relation to other information assets.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
7.5.2	Change Management	A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover factors such as security and implications of the change in relation to other information assets.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
7.5.3	Change Management	The FI should ensure all changes are adequately tested in the test environment. Test plans for changes should be developed and approved by the relevant business and IT management. Test results should be accepted and signed off before the changes are deployed to the production environment.	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	
7.5.4	Change Management	A change advisory board, comprising key stakeholders including business and IT management, should be formed to approve and prioritise the changes after considering the stability and security implications of the changes to the production environment.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
7.5.5	Change Management	The FI should perform a backup of the information asset prior to the change implementation, and establish a rollback plan to revert the information asset to the previous state if a problem arises during or after the change implementation.	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	
7.5.6	Change Management	Urgent or emergency changes, such as a high priority security patch for an IT system, are changes that need to be implemented expeditiously and may not be able to follow the standard change management process. To reduce the risk to the security and stability of the production environment, the FI should clearly define the procedures for assessing, approving and implementing emergency changes, as well as identify the authorisers or approvers for the changes.	Functional	Intersects With	Emergency Changes	CHG-07	Mechanisms exist to govern change management procedures for "emergency" changes.	5	
7.5.7	Change Management	Logs contain useful information which facilitates investigations and troubleshooting. As such, the FI should ensure the logging facility is enabled to record activities that are performed during the change process.	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	
7.6	Software Release Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.6.1	Software Release Management	Segregation of duties in the software release process should be practised to ensure no single individual has the ability to develop, compile and move software codes11 from one environment to another.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
7.6.2	Software Release Management	It is important that controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.	Functional	Intersects With	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	5	
7.6.2	Software Release Management	It is important that controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
7.6.2	Software Release Management	It is important that controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
7.7	Incident Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.7.1	Incident Management	An IT incident occurs when there is an unexpected disruption to the delivery of IT services or a security breach of an IT system, which compromises the confidentiality, integrity and availability of data or the IT system. The FI should establish an incident management framework with the objective of restoring an affected IT service or system to a secure and stable state, as quickly as possible, so as to minimise impact to the FI's business and customers.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7.7.2	Incident Management	The FI should ensure sufficient resources are available to facilitate and support incident response and recovery. The FI may engage external assistance to augment its resources to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber attack investigation, and provide 24 by 7 incident response capability.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.7.2	Incident Management	The FI should ensure sufficient resources are available to facilitate and support incident response and recovery. The FI may engage external assistance to augment its resources to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber attack investigation, and provide 24 by 7 incident response capability.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
7.7.3	Incident Management	The incident management framework should minimally cover:	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.7.3(a)	Incident Management	the process and procedure for handling IT incidents, including cyber related incidents; 12	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.7.3(b)	Incident Management	maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.7.3(c)	Incident Management	the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.7.4	Incident Management	The FI should configure system events or alerts to provide an early indication of issues that may affect its IT systems' performance and security. System events or alerts should be actively monitored so that prompt measures can be taken to address the issues early.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
7.7.5	Incident Management	In some situations, a major incident may develop unfavourably into a crisis. The FI should regularly apprise its senior management of the status of major incidents so that decisions to mitigate the impact of the crisis can be made in a timely manner, such as activation of IT disaster recovery.	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 and data protection incident response operations.	8	
7.7.5	Incident Management	In some situations, a major incident may develop unfavourably into a crisis. The FI should regularly apprise its senior management of the status of major incidents so that decisions to mitigate the impact of the crisis can be made in a timely manner, such as activation of IT disaster recovery.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3	
7.7.6	Incident Management	A communications plan that covers the process and procedures to apprise customers of impact on services, and to handle media or public queries should be maintained. The plan should also include identifying the spokespersons and subject matter experts to address the media or public queries as well as the communication channels to disseminate information.	Functional	Subset Of	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 and data protection incident response operations.	10	
7.7.7	Incident Management	It would be useful for the FI to provide timely updates to its customers on the progress of its incident management and the measures the FI is implementing to protect its customers and continue delivery of financial services. Where appropriate, the FI should advise its customers on actions that they should take to protect themselves.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
7.8	Problem Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.8.1	Problem Management	The FI should establish problem management process and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
7.8.2	Problem Management	The FI should maintain a record of past incidents which include lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
7.8.3	Problem Management	A trend analysis of past incidents should be performed by the FI to identify commonalities and patterns in the incidents, and verify if the root causes to the problems had been properly identified and resolved. The FI should also use the analysis to determine if further corrective or preventive measures are necessary.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	5	
8	IT Resilience	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.1	System Availability	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.1.1	System Availability	Maintaining system availability is crucial in achieving confidence and trust in the FI's operational capabilities. IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
8.1.2	System Availability	Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. The review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
8.1.2	System Availability	Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. The review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
8.1.2	System Availability	Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. The review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.	Functional	Intersects With	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	5	
8.1.3	System Availability	The FI should continuously monitor the utilisation of its system resources against a set of pre-defined thresholds. 13 Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet 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 Technology Assets, Applications and/or Services (TAAS).	8	
8.1.4	System Availability	Procedures should be established to respond to situations when pre-defined thresholds for system resources and system performance have been breached.	Functional	Intersects With	Elastic Expansion	CAP-05	Mechanisms exist to automatically scale the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.	3	
8.2	System Recoverability	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.2.1	System Recoverability	The FI should establish systems' recovery time objectives (RTO) and recovery point objectives (RPO) that are aligned to its business resumption and system recovery priorities.	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).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.2.2	System Recoverability	The FI's disaster recovery plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of relevant personnel in the recovery process. The disaster recovery plan should be reviewed at least annually and updated when there are material changes to business operations, information assets or environmental factors.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
8.2.3	System Recoverability	During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management. The FI should avoid deviating from the plan as untested recovery measures could exacerbate the incident and prolong the recovery process. In exceptional circumstances where untested recovery measures need to be used, the FI should perform a risk assessment and ensure adequate controls are in place, as well as obtain approval from senior management.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	
8.2.4	System Recoverability	The FI should endeavour to operate from its recovery, secondary or alternate site periodically so as to have the assurance that its infrastructure and systems at these sites are able to support business needs for an extended period of time when production systems failover from the primary or production site.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	
8.3	Testing of Disaster Recovery Plan	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.3.1	Testing of Disaster Recovery Plan	The FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the defined recovery objectives. Relevant stakeholders, including those in business and IT functions, should participate in the disaster recovery test to familiarise themselves with the recovery processes and ascertain if the systems are performing as expected.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
8.3.2	Testing of Disaster Recovery Plan	A disaster recovery test plan should include the test objectives and scope, test scenarios, test scripts with details of the activities to be performed during and after testing, system recovery procedures, and the criteria for measuring the success of the test.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
8.3.3	Testing of Disaster Recovery Plan	The testing of disaster recovery plan should comprise:	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
8.3.3(a)	Testing of Disaster Recovery Plan	various plausible disruption scenarios, including full and partial incapacitation of the primary or production site and major system failures; and	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
8.3.3(b)	Testing of Disaster Recovery Plan	recovery dependencies between information assets, including those managed by third parties.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
8.3.4	Testing of Disaster Recovery Plan	Where information assets are managed by service providers, the FI should assess the service provider's disaster recovery capability and ensure disaster recovery arrangements for these information assets are established, tested and verified to meet its business needs. The FI should engage its service provider to test the recovery steps that require coordinated actions between the service provider and the FI.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
8.3.4	Testing of Disaster Recovery Plan	Where information assets are managed by service providers, the FI should assess the service provider's disaster recovery capability and ensure disaster recovery arrangements for these information assets are established, tested and verified to meet its business needs. The FI should engage its service provider to test the recovery steps that require coordinated actions between the service provider and the FI.	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
8.4	System Backup and Recovery	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.4.1	System Backup and Recovery	The FI should establish a system and data backup strategy, and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
8.4.2	System Backup and Recovery	To ensure data availability is aligned with the FI's business requirements, the FI should institute a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
8.4.3	System Backup and Recovery	The FI should periodically test the restoration of its system and data backups to validate the effectiveness of its backup restoration procedures.	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
8.4.4	System Backup and Recovery	To protect data in backup from unauthorised access and modification, the FI should ensure any confidential data stored in the backup media is secured (e.g. encrypted). Backup media should be stored offline or at an offsite location.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
8.4.4	System Backup and Recovery	To protect data in backup from unauthorised access and modification, the FI should ensure any confidential data stored in the backup media is secured (e.g. encrypted). Backup media should be stored offline or at an offsite location.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
8.5	Data Centre Resilience	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
8.5.1	Data Centre Resilience	The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres(DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. 14 In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
8.5.1	Data Centre Resilience	The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres(DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. 14 In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.	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.	8	
8.5.1	Data Centre Resilience	The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres(DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. 14 In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	3	
8.5.2	Data Centre Resilience	The FI should ensure adequate redundancy for the power, network connectivity, and cooling, electrical and mechanical systems of the DC to eliminate any single point of failure. Consideration should be given to the following:	Functional	Intersects With	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	
8.5.2(a)	Data Centre Resilience	diversification of data communications and network paths;	Functional	Intersects With	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	
8.5.2(b)	Data Centre Resilience	deployment of power equipment, such as uninterruptable power sources, backup diesel generators with fuel tanks; and	Functional	Intersects With	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	
8.5.2(c)	Data Centre Resilience	implementation of redundant cooling equipment (e.g. cooling towers, chilled water supply and computer room air conditioning units) to control the temperature and humidity levels in the DC and prevent fluctuations potentially harmful to systems.	Functional	Intersects With	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	5	
8.5.3	Data Centre Resilience	As part of the DC's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems.	Functional	Intersects With	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.5.3	Data Centre Resilience	As part of the DC's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems.	Functional	Intersects With	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	5	
8.5.3	Data Centre Resilience	As part of the DC's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems.	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	5	
8.5.4	Data Centre Resilience	The FI's secondary or disaster recovery DC should be geographically separated from its primary or production DC so that both sites will not be impacted by a disruption to the underlying infrastructure (e.g. telecommunications and power) in a particular location.	Functional	Intersects With	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	
8.5.5	Data Centre Resilience	The DC's physical security and environmental controls should be monitored on a 24 by 7 basis. Appropriate escalation, response plans and procedures for physical and environmental incidents at DCs should be established and tested.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
8.5.6	Data Centre Resilience	The DC should have adequate physical access controls including:	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
8.5.6(a)	Data Centre Resilience	access granted to staff should be on a need-to-have basis, and revoked promptly if access is no longer required;	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
8.5.6(b)	Data Centre Resilience	proper notification and approval for visitors to the DC. All visitors should be escorted by authorised staff at all times while in the DC;	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
8.5.6(c)	Data Centre Resilience	physical access points in the DC should be secured and monitored at all times;	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
8.5.6(d)	Data Centre Resilience	access to equipment racks should be restricted to authorised staff and monitored;	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5	
8.5.6(e)	Data Centre Resilience	access to keys and other physical access devices should be restricted to authorised staff, and replaced or changed promptly if they have been misplaced, lost or stolen; and	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	
8.5.6(f)	Data Centre Resilience	segregation of delivery and common areas from security sensitive areas should be enforced.	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	
9	Access Control	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
9.1	User Access Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
9.1.1	User Access Management	The principles of 'never alone', 15 'segregation of duties', 16 and 'least privilege' 17 should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions. 18 Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	
9.1.1	User Access Management	The principles of 'never alone', 15 'segregation of duties', 16 and 'least privilege' 17 should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions. 18 Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
9.1.2	User Access Management	The FI should establish a user access management process19 to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
9.1.3	User Access Management	For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.	Functional	Intersects With	Retain Access Records	IAC-01.1	Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed.	5	
9.1.4	User Access Management	The FI should establish a password policy and a process to enforce strong password controls20 for users' access to IT systems.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
9.1.5	User Access Management	Multi-factor authentication21 should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorised access.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
9.1.6	User Access Management	The FI should ensure appropriate parties such as information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
9.1.7	User Access Management	Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
9.1.7	User Access Management	Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
9.1.8	User Access Management	The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
9.1.8	User Access Management	The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
9.2	Privileged Access Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
9.2.1	Privileged Access Management	Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
9.2.2	Privileged Access Management	System and service accounts are used by operating systems, applications and databasesto interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
9.2.2	Privileged Access Management	System and service accounts are used by operating systems, applications and databasesto interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	8	
9.3	Remote Access Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9.3.1	Remote Access Management	Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
9.3.2	Remote Access Management	The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
10	Cryptography	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
10.1	Cryptographic Algorithm and Protocol	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
10.1.1	Cryptographic Algorithm and Protocol	The primary applications of cryptography are to protect data confidentiality, and maintain data integrity and authenticity. For example, cryptography is used in data encryption to protect sensitive data; cryptographic digital signatures can be used to verify the authenticity of the data origin and check if the data has been altered. Besides these applications, cryptography is also commonly used in authentication protocols.	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	
10.1.2	Cryptographic Algorithm and Protocol	The FI should adopt cryptographic algorithms from well-established international standards. The FI should also select an appropriate algorithm and encryption key length that meet its security objectives and requirements.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5	
10.1.3	Cryptographic Algorithm and Protocol	Where the security of the cryptographic algorithm depends on the unpredictability of a random seed or number, the FI should ensure the seed or random number is of sufficient length and randomness.	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	
10.1.4	Cryptographic Algorithm and Protocol	The FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.	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	
10.1.5	Cryptographic Algorithm and Protocol	The FI should monitor developments in the area of cryptanalysis and, where necessary, update or change the cryptographic algorithms or increase the key lengths to ensure they remain resilient against evolving threats.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5	
10.2	Cryptographic Key Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
10.2.1	Cryptographic Key Management	Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.2	Cryptographic Key Management	The FI should ensure cryptographic keys are securely generated and protected from unauthorised disclosure. Any cryptographic key or sensitive data used to generate or derive the keys should be also be protected or securely destroyed after the key is generated.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.3	Cryptographic Key Management	The FI should determine the appropriate lifespan of each cryptographic key based on factors, such as the sensitivity of the data, the criticality of the system to be protected, and the threats and risks that the data or system may be exposed to. The cryptographic key should be securely replaced, before it expires at the end of its lifespan.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.4	Cryptographic Key Management	To protect sensitive cryptographic keys, the FI should manage, process and store such keys in hardened and tamper resistant systems, e.g. by using a hardware security module.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.5	Cryptographic Key Management	Where sensitive cryptographic keys need to be transmitted, the FI should ensure these keys are not exposed during transmission. The keys should be distributed to the intended recipient via an out-of-band channel or other secure means to minimise the risk of interception.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.6	Cryptographic Key Management	Diversification of cryptographic keys can limit the impact of key exposure. Cryptographic keys should be used for a single purpose. For instance, the cryptographic key for data encryption should be different from the one that is used to generate cryptographic digital signatures.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.7	Cryptographic Key Management	If a cryptographic key is found to be compromised, the FI should revoke and replace the key and all other keys whose security could also be compromised as a result of the exposed key.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
10.2.8	Cryptographic Key Management	When cryptographic keys have expired or have been revoked, the FI should use a secure key destruction method to ensure the keys are not recoverable.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
10.2.9	Cryptographic Key Management	When replacing or renewing a compromised or expiring cryptographic key, the FI should generate the new key in a manner such that any adversary who has knowledge of part or whole of the previous key will not be able to derive the new key from it.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
10.2.10	Cryptographic Key Management	Cryptographic keys can be corrupted or unintentionally deleted. As such, the FI should maintain backups of cryptographic keys for recovery purposes and accord them a high level of protection.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
11	Data and Infrastructure Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.1	Data Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.1.1	Data Security	The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
11.1.1	Data Security	The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
11.1.1	Data Security	The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:	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	
11.1.1(a)	Data Security	data in motion - data that traverses a network or that is transported between sites;	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
11.1.1(b)	Data Security	data at rest - data in endpoint devices such as notebooks, personal computers, portable storage devices and mobile devices, as well as data in systems such as files stored on servers, databases, backup media and storage platforms (e.g. cloud); and	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
11.1.1(c)	Data Security	data in use - data that is being used or processed by a system.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
11.1.2	Data Security	The FI should implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices. The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
11.1.3	Data Security	Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
11.1.3	Data Security	Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
11.1.4	Data Security	The FI should ensure only authorised data storage media, systems and endpoint devices are used to communicate, transfer, or store confidential data.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
11.1.4	Data Security	The FI should ensure only authorised data storage media, systems and endpoint devices are used to communicate, transfer, or store confidential data.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11.1.5	Data Security	Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.1.5	Data Security	Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
11.1.5	Data Security	Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
11.1.6	Data Security	The use of sensitive production data in non-production environments should be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval has to be obtained from senior management. The FI should ensure appropriate controls are implemented in non-production environments to manage the access and removal of such data to prevent data leakage. Where possible, such data should be masked in the non-production environments.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
11.1.6	Data Security	The use of sensitive production data in non-production environments should be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval has to be obtained from senior management. The FI should ensure appropriate controls are implemented in non-production environments to manage the access and removal of such data to prevent data leakage. Where possible, such data should be masked in the non-production environments.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.	5	
11.1.7	Data Security	The FI should ensure confidential data is irrevocably deleted from storage media, systems and endpoint devices before they are disposed of or redeployed.	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	
11.1.7	Data Security	The FI should ensure confidential data is irrevocably deleted from storage media, systems and endpoint devices before they are disposed of or redeployed.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
11.2	Network Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.2.1	Network Security	The FI should install network security devices such as firewalls to secure the network between the FI and the Internet, as well as connections with third parties.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
11.2.1	Network Security	The FI should install network security devices such as firewalls to secure the network between the FI and the Internet, as well as connections with third parties.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	8	
11.2.2	Network Security	To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and application) or the sensitivity of the data.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	8	
11.2.3	Network Security	Network intrusion prevention systems should be deployed in the FI's network to detect and block malicious network traffic.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	8	
11.2.4	Network Security	The FI should implement network access controls to detect and prevent unauthorised devices from connecting to its network.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	8	
11.2.5	Network Security	Network access control rules in network devices such as firewalls, routers, switches and access points should be reviewed on a regular basis to ensure they are kept up-to-date. Obsolete rules and insecure network protocols should be removed promptly as these can be exploited to gain unauthorised access to the FI's network and systems.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5	
11.2.6	Network Security	Internet web browsing provides a conduit for cyber criminals to access the FI's IT systems. In this regard, the FI should consider isolating internet web browsing activities from its endpoint devices through the use of physical or logical controls, or implement equivalent controls, so as to reduce exposure of its IT systems to cyber attacks.	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	
11.2.7	Network Security	An effective DoS protection should be implemented to detect and respond to various types of DoS attacks. 22 The FI could engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI's network infrastructure.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
11.2.8	Network Security	A review of the FI's network architecture, including the network security design, as well as system and network interconnections, should be conducted on a periodic basis to identify potential cyber security vulnerabilities.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
11.2.8	Network Security	A review of the FI's network architecture, including the network security design, as well as system and network interconnections, should be conducted on a periodic basis to identify potential cyber security vulnerabilities.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
11.3	System Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.3.1	System Security	The security standards for the FI's hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
11.3.2	System Security	The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
11.3.2	System Security	The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
11.3.3	System Security	Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	3	
11.3.4	System Security	The FI should ensure that anti-malware signatures are kept up-to-date and the systems are regularly scanned for malicious files or anomalous activities.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
11.3.5	System Security	To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.	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	
11.3.5	System Security	To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
11.3.6	System Security	Security measures, such as application white-listing, should be implemented to ensure only authorised software is allowed to be installed on the FI's systems.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11.3.7	System Security	When implementing Bring Your Own Device (BYOD) 23, the FI should conduct a comprehensive risk assessment and implement appropriate measures to secure its BYOD environment before allowing staff to use their personal devices to access the corporate network. Refer to Annex B on the security measures for BYOD.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
11.4	Virtualisation Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.4.1	Virtualisation Security	Virtualisation 24 is used by organisations to optimise the use of computing resources and to enhance resilience. The technology allows several virtual machines (VMs) that support different business applications to be hosted on a physical system. A system failure or security breach in one of the VMs could have contagion impact on other VMs. The FI should ensure security standards are established for all components25 of a virtualisation solution.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
11.4.2	Virtualisation Security	Strong access controls should be implemented to restrict administrative access to the hypervisor and host operating system as both control the guest operating systems and other components in the virtual environment.	Functional	Intersects With	Hypervisor Access	END-15	Mechanisms exist to restrict access to hypervisor management functions or administrative consoles for systems hosting virtualized systems.	5	
11.4.3	Virtualisation Security	The FI should establish policies and standards to manage virtual images and snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorised access or modification.	Functional	Intersects With	Recovery Images	BCD-11.3	Mechanisms exist to reimage assets from configuration-controlled and integrity-protected images that represent a secure, operational state.	5	
11.4.3	Virtualisation Security	The FI should establish policies and standards to manage virtual images and snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorised access or modification.	Functional	Intersects With	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	5	
11.4.3	Virtualisation Security	The FI should establish policies and standards to manage virtual images and snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorised access or modification.	Functional	Intersects With	Virtual Machine Images	CLD-05	Mechanisms exist to ensure the integrity of virtual machine images at all times.	5	
11.5	Internet of Things	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
11.5.1	Internet of Things	Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which can be connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, including information such as the networks which they are connected to and their physical locations.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
11.5.1	Internet of Things	Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which can be connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, including information such as the networks which they are connected to and their physical locations.	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
11.5.2	Internet of Things	Many IoT devices are designed without or with minimal security controls. If compromised, these devices can be commandeered and used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT.	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
11.5.3	Internet of Things	The network that hosts IoT devices should be secured. For instance, network access controls can be implemented to restrict network traffic to and from an IoT device to prevent a cyber threat actor from accessing the FI's network and launching malware or DoS attacks. To further reduce IoT risks, the FI should host IoT devices in a separate network segment from the network that hosts the FI's systems and confidential data.	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
11.5.4	Internet of Things	The FI should implement controls to prevent unauthorised access to IoT devices.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5	
11.5.5	Internet of Things	Similar to other systems, the FI should monitor IoT devices for suspicious or anomalous system activities so that prompt actions can be taken to isolate compromised devices.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
11.5.5	Internet of Things	Similar to other systems, the FI should monitor IoT devices for suspicious or anomalous system activities so that prompt actions can be taken to isolate compromised devices.	Functional	Intersects With	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.	5	
12	Cyber Security Operations	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
12.1	Cyber Threat Intelligence and Information Sharing	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
12.1.1	Cyber Threat Intelligence and Information Sharing	To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
12.1.2	Cyber Threat Intelligence and Information Sharing	The FI should procure cyber intelligence monitoring services. As cyber threat information sharing is an important component of cyber resilience within the financial ecosystem, the FI should actively participate in cyber threat information-sharing arrangements with trusted partiesto share and receive timely and actionable cyber threat information.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
12.1.3	Cyber Threat Intelligence and Information Sharing	At the same time, the FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the Internet. The FI should consider engaging external media monitoring services to facilitate the evaluation and identification of online misinformation.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	3	
12.1.3	Cyber Threat Intelligence and Information Sharing	At the same time, the FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the Internet. The FI should consider engaging external media monitoring services to facilitate the evaluation and identification of online misinformation.	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
12.2	Cyber Event Monitoring and Detection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
12.2.1	Cyber Event Monitoring and Detection	To facilitate continuous monitoring and analysis of cyber events; 26 as well as prompt detection and response to cyber incidents, the FI should establish a security operations centre or acquire managed security services. The processes, roles and responsibilities for security operations should be defined.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
12.2.2	Cyber Event Monitoring and Detection	A process to collect, process, review and retain system logs 27 should be established to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
12.2.2	Cyber Event Monitoring and Detection	A process to collect, process, review and retain system logs 27 should be established to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
12.2.3	Cyber Event Monitoring and Detection	To facilitate identification of anomalies, the FI should establish a baseline profile of each IT system's routine activities and analyse the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
12.2.3	Cyber Event Monitoring and Detection	To facilitate identification of anomalies, the FI should establish a baseline profile of each IT system's routine activities and analyse the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
12.2.4	Cyber Event Monitoring and Detection	The FI should consider applying user behavioural analytics to enhance the effectiveness of security monitoring. User behavioural analytics might include the use of machine learning algorithms in real time to analyse system logs, establish a baseline of normal user activities and identify suspicious or anomalous behaviours.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
12.2.5	Cyber Event Monitoring and Detection	Correlation of multiple events registered on system logs should be performed to identify suspicious or anomalous system activity patterns.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
12.2.6	Cyber Event Monitoring and Detection	A process should be established to ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behaviour.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
12.3	Cyber Incident Response and Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
12.3.1	Cyber Incident Response and Management	The FI should establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to securely resume affected services. The plan should describe communication, coordination and response procedures to address plausible cyber threat scenarios.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
12.3.2	Cyber Incident Response and Management	As part of the plan, the FI should establish a process to investigate and identify the security or control deficiencies that resulted in the security breach. The investigation should also evaluate the full extent of the impact to the FI.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
12.3.3	Cyber Incident Response and Management	Information from cyber intelligence and lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	5	
13	Cyber Security Assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.1	Vulnerability Assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.1.1	Vulnerability Assessment	The FI should establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the IT system and the security risk to which it is exposed.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
13.1.2	Vulnerability Assessment	When performing VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, and open network ports, as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
13.2	Penetration Testing	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.2.1	Penetration Testing	The FI should carry out penetration testing (PT) 28 to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
13.2.2	Penetration Testing	A bug bounty programme is another means by which an FI could discover vulnerabilities in their IT systems by inviting and incentivising ethical or "white hat" hackers to conduct PT on their systems. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT.	Functional	Subset Of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	10	
13.2.3	Penetration Testing	To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
13.2.4	Penetration Testing	The frequency of PT should be determined based on factors such as system criticality and the system's exposure to cyber risks. For systems that are directly accessible from the Internet, the FI is expected to conduct PT to validate the adequacy of the security controls at least once annually or whenever these systems undergo major changes or updates.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
13.3	Cyber Exercises	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.3.1	Cyber Exercises	The FI should carry out regular scenario-based cyber exercises to validate its response and recovery, as well as communication plans against cyber threats. These exercises could include social engineering, 29 table-top, 30 or cyber range31 exercises.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
13.3.2	Cyber Exercises	Depending on the exercise objectives, the FI should involve relevant stakeholders, including senior management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
13.4	Adversarial Attack Simulation Exercise	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.4.1	Adversarial Attack Simulation Exercise	The FI should perform an adversarial attack simulation exercise32 to test and validate the effectiveness of its cyber defence and response plan against prevalent cyber threats.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
13.4.2	Adversarial Attack Simulation Exercise	The objectives, scope and rules of engagement should be defined before the commencement of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team33 do not disrupt the FI's production systems.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
13.5	Intelligence-Based Scenario Design	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.5.1	Intelligence-Based Scenario Design	To simulate realistic adversarial attacks during any cyber security assessment, the threat scenario should be designed and based on challenging but plausible cyber threats.	Functional	Intersects With	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	5	
13.5.2	Intelligence-Based Scenario Design	The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.	Functional	Intersects With	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	5	
13.5.2	Intelligence-Based Scenario Design	The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
13.5.2	Intelligence-Based Scenario Design	The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
13.6	Remediation Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
13.6.1	Remediation Management	A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises. The process should minimally include the following:	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
13.6.1(a)	Remediation Management	severity assessment and classification of an issue;	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
13.6.1(b)	Remediation Management	timeframe to remediate issues of different severity; and	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
13.6.1(c)	Remediation Management	risk assessment and mitigation strategies to manage deviations from the framework.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
14	Online Financial Services	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
14.1	Security of Online Financial Services	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
14.1.1	Security of Online Financial Services	Online financial services include banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. 34 In delivering online financial services, the FI should implement security and control measures which are commensurate with the risk involved to ensure the security of data and online services.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
14.1.1	Security of Online Financial Services	Online financial services include banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. 34 In delivering online financial services, the FI should implement security and control measures which are commensurate with the risk involved to ensure the security of data and online services.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	5	
14.1.1	Security of Online Financial Services	Online financial services include banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. 34 In delivering online financial services, the FI should implement security and control measures which are commensurate with the risk involved to ensure the security of data and online services.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.1.2	Security of Online Financial Services	The FI should secure its communications channels to protect customer data. This can be achieved through data encryption and digital signatures.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.1.3	Security of Online Financial Services	Adequate measures should also be taken to minimise exposure of the FI's online financial services to common attack vectors such as code injection attack, cross-site scripting, man-in-the-middle attack (MITMA), 35 domain name system (DNS) hijacking, 36 distributed denial of service (DDoS), malware and spoofing attacks.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.1.4	Security of Online Financial Services	An FI offering online financial services access via a mobile device should be aware of the risks unique to mobile applications. Specific measures aimed at addressing the risks of mobile applications should be put in place. Refer to Annex C for guidance on Mobile Application Security.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.1.5	Security of Online Financial Services	The FI should only make available mobile applications or software to customers through official mobile application stores, or other secure delivery channels.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
14.1.6	Security of Online Financial Services	The FI should actively monitor for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report phishing attempts to service providers to facilitate the removal of malicious content. The FI should alert its customers of such campaigns and advise them of security measures to adopt to protect against phishing.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
14.1.6	Security of Online Financial Services	The FI should actively monitor for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report phishing attempts to service providers to facilitate the removal of malicious content. The FI should alert its customers of such campaigns and advise them of security measures to adopt to protect against phishing.	Functional	Intersects With	Dynamic Threat Awareness	THR-01.1	Mechanisms exist to determine and maintain ongoing awareness of the current cyber threat environment.	5	
14.1.7	Security of Online Financial Services	Rooted or jailbroken mobile devices, which are more susceptible to malware and may have more security vulnerabilities, should be disallowed from accessing the FI's mobile applications to perform financial transactions unless the application has been secured within a sandbox or container that insulates the application from tampering and interception by malware.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
14.2	Customer Authentication and Transaction Signing	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
14.2.1	Customer Authentication and Transaction Signing	Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. one-time password (OTP) generator) and who you are (e.g. biometrics).	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.2.1	Customer Authentication and Transaction Signing	Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. one-time password (OTP) generator) and who you are (e.g. biometrics).	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.2	Customer Authentication and Transaction Signing	End-to-end encryption should be implemented for the transmission of customer passwords so that they are not exposed at any intermediate nodes between the customer mobile application or browser and the IT system where passwords are verified. To safeguard the confidentiality of customer passwords, the passwords should only be verified in a hardened or tamper resistant system.	Functional	Intersects With	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5	
14.2.3	Customer Authentication and Transaction Signing	The FI should implement transaction-signing (e.g. digital signatures) for authorising high-risk activities to protect the integrity of customer accounts' data and transaction details. High-risk activities include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details, high value funds transfers and revision of funds transfer limits.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.2.4	Customer Authentication and Transaction Signing	Besides login and transaction-signing for high-risk activities, the FI may implement appropriate risk-based or adaptive authentication that presents customers with authentication options that are commensurate with the risk level of the transaction and sensitivity of the data.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.2.5	Customer Authentication and Transaction Signing	When implementing time-based OTPs, the FI should establish a validity period that is as short as practicable to lower the risk of a stolen OTP being used for fraudulent transactions.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.6	Customer Authentication and Transaction Signing	Where biometric technologies37 and customer passwords are used for customer authentication, the FI should ensure the biometrics-related data and authentication credentials are encrypted in storage and during transmission.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.7	Customer Authentication and Transaction Signing	The performance ofthe biometric solution, based on false acceptance rate(FAR)38 and false rejection rate (FRR), 39 should be calibrated to be commensurate with the risk associated with the online activity.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.8	Customer Authentication and Transaction Signing	A soft token is a software-based two-factor authentication mechanism installed on a general-purpose device.40 Appropriate measures, such as verifying the identity of the customer, detecting and blocking rooted or jailbroken devices, and performing device binding,41 should be implemented during soft token provisioning.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.9	Customer Authentication and Transaction Signing	The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. Measures to detect and terminate hijacked sessions should be implemented. To reduce the risk of an attacker from maintaining a hijacked session indefinitely, an online session should be automatically terminated after inactivity for a pre-defined time.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
14.2.10	Customer Authentication and Transaction Signing	Where alternate controls and processes (e.g. maker-checker function) are implemented for corporate or institutional customers to authorise transactions, the FI should perform a security risk assessment of controls or processes to ensure they are commensurate with the risk of the activities that are being carried out.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Monitory Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines (2021)
Focal Document URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-mas-trm-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
14.2.11	Customer Authentication and Transaction Signing	To safeguard the confidentiality of authentication credentials, such as biometric templates and passwords, the FI should store these credentials in a form that is resistant to reverse engineering. A process and procedure should also be implemented to revoke and replace authentication credentials and mechanisms that have been compromised.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
14.3	Fraud Monitoring	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
14.3.1	Fraud Monitoring	The FI should implement real-time fraud monitoring systems to identify and block suspicious or fraudulent online transactions. 42	Functional	No Relationship	N/A	N/A	N/A	0	
14.3.2	Fraud Monitoring	A process should be established to investigate suspicious transactions or payments and to ensure issues are adequately and promptly addressed.	Functional	No Relationship	N/A	N/A	N/A	0	
14.3.3	Fraud Monitoring	The FI should notify customers of suspicious activities or funds transfers above a threshold that is defined by the FI or customers. The notification should contain meaningful information such as type of transaction and payment amount, as well as instructions to report suspicious activities or unauthorised transactions.	Functional	No Relationship	N/A	N/A	N/A	0	
14.4	Customer Education and Communication	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
14.4.1	Customer Education and Communication	Customers should be informed of the security best practices that they should adopt when using online financial services. This includes the measures to take to secure their electronic devices that are used to access online financial services.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	3	
14.4.2	Customer Education and Communication	The FI should alert its customers on a timely basis to new cyber threats so that they can take precautionary measures.	Functional	No Relationship	N/A	N/A	N/A	0	
14.4.3	Customer Education and Communication	The FI should advise their customers on the means to detect unauthorised transactions and to report promptly security issues, suspicious activities or suspected fraud to the FI.	Functional	No Relationship	N/A	N/A	N/A	0	
15	IT Audit	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
15.1	Audit Function	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
15.1.1	Audit Function	Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FI. The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology risks.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
15.1.1	Audit Function	Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FI. The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology risks.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
15.1.2	Audit Function	A comprehensive set of auditable areas for technology risk should be identified so that an effective risk assessment could be performed during audit planning. Auditable areas should include all IT operations, functions and processes.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
15.1.3	Audit Function	The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
15.1.4	Audit Function	The FI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-01.6	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5	