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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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	Introduction	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2	Framework Structure and Features	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3	Control domains	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.1	Cyber Security Leadership and Governance	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.1.1	Cyber Security Governance	A cyber security governance structure should be defined and implemented, and should be endorsed by the board.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
3.1.1.1	Cyber Security Governance	A cyber security committee should be established and be mandated by the board.	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	
3.1.1.2	Cyber Security Governance	The cyber security committee should be headed by an independent senior manager from a control function.	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	
3.1.1.3	Cyber Security Governance	The following positions should be represented in the cyber security committee:	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	
3.1.1.3.a	Cyber Security Governance	senior managers from all relevant departments (e.g., COO, CIO, compliance officer, heads of relevant business departments);	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	
3.1.1.3.b	Cyber Security Governance	Chief information security officer (CISO);	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	
3.1.1.3.c	Cyber Security Governance	Internal audit may attend as an "observer.	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	
3.1.1.4	Cyber Security Governance	A cyber security committee charter should be developed, approved and reflect:	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	
3.1.1.4.a	Cyber Security Governance	committee objectives;	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	
3.1.1.4.b	Cyber Security Governance	roles and responsibilities;	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	
3.1.1.4.c	Cyber Security Governance	minimum number of meeting participants;	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	
3.1.1.4.d	Cyber Security Governance	meeting frequency (minimum on quarterly basis).	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	
3.1.1.5	Cyber Security Governance	A cyber security function should be established.	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	
3.1.1.6	Cyber Security Governance	A cyber security function should be established. 6. The cyber security function should be independent from	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	
3.1.1.7	Cyber Security Governance	The cyber security function should report directly to the CEO/managing director of the Member Organization or general manager of a control function.	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	
3.1.1.8	Cyber Security Governance	A full-time senior manager for the cyber security function, referred to as CISO, should be appointed at senior management level.	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	
3.1.1.9	Cyber Security Governance	The Member Organization should :	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	
3.1.1.9.a	Cyber Security Governance	ensure the CISO has a Saudi nationality;	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	
3.1.1.9.b	Cyber Security Governance	ensure the CISO is sufficiently qualified;	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	
3.1.1.9.c	Cyber Security Governance	obtain no objection from SAMA to assign the CISO.	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	
3.1.1.10	Cyber Security Governance	The board of the Member Organization should allocate sufficient budget to execute the required cyber security activities.	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5	
3.1.2	Cyber Security Strategy	A cyber security strategy should be defined and aligned with the Member Organization's strategic objectives, as well as with the Banking Sector's cyber security strategy.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.1	Cyber Security Strategy	The cyber security strategy should be defined, approved, maintained and executed.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.1.2.2	Cyber Security Strategy	The cyber security strategy should be aligned with:	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.2.a	Cyber Security Strategy	the Member Organization's overall objectives;	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.2.b	Cyber Security Strategy	the legal and regulatory compliance requirements of the Member Organization;	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.2.c	Cyber Security Strategy	the Banking Sector's cyber security strategy.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.3	Cyber Security Strategy	The cyber security strategy should address:	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.3.a	Cyber Security Strategy	the importance and benefits of cyber security for the Member Organization;	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.3.b	Cyber Security Strategy	the anticipated future state of cyber security for the Member Organization to become and remain resilient to (emerging) cyber security threats;	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.2.3.c	Cyber Security Strategy	which and when cyber security initiatives and projects should be executed to achieve the anticipated future state	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
3.1.3	Cyber Security Policy	A cyber security policy should be defined, approved and communicated.	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	
3.1.3.1	Cyber Security Policy	The cyber security policy should be defined, approved and communicated.	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	
3.1.3.2	Cyber Security Policy	The cyber security policy should be reviewed periodically according to a predefined and structured review process.	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	
3.1.3.3	Cyber Security Policy	The cyber security policy should be:	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	
3.1.3.3.a	Cyber Security Policy	considered as input for other corporate policies of the Member Organization (e.g., HR policy, finance policy and IT policy);	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	
3.1.3.3.b	Cyber Security Policy	supported by detailed security standards (e.g., password standard, firewall standard) and procedures;	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	
3.1.3.3.c	Cyber Security Policy	based on best practices and (inter)national standards;	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	
3.1.3.3.d	Cyber Security Policy	communicated to relevant stakeholders.	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	
3.1.3.4	Cyber Security Policy	The cyber security policy should include:	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	
3.1.3.4.a	Cyber Security Policy	a definition of cyber security;	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	
3.1.3.4.b	Cyber Security Policy	the Member Organization's overall cyber security objectives and scope;	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	
3.1.3.4.c	Cyber Security Policy	a statement of the board's intent, supporting the cyber security objectives;	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	
3.1.3.4.d	Cyber Security Policy	a definition of general and specific responsibilities for cyber security;	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	
3.1.3.4.e	Cyber Security Policy	the reference to supporting cyber security standards and procedures;	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	
3.1.3.4.f	Cyber Security Policy	cyber security requirements that ensure:	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	
3.1.3.4.f.1	Cyber Security Policy	information is classified in a way that indicates its importance to the Member Organization;	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	
3.1.3.4.f.2	Cyber Security Policy	information is protected in terms of cyber security requirements, in line with the risk appetite;	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	
3.1.3.4.f.3	Cyber Security Policy	owners are appointed for all information assets;	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	
3.1.3.4.f.4	Cyber Security Policy	cyber security risk assessments are conducted for information assets;	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	
3.1.3.4.f.5	Cyber Security Policy	relevant stakeholders are made aware of cyber security and their expected behavior (cyber security awareness program);	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	
3.1.3.4.f.6	Cyber Security Policy	compliance with regulatory and contractual obligations are being met;	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	
3.1.3.4.f.7	Cyber Security Policy	cyber security breaches and suspected cyber security weaknesses are reported;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.1.3.4.f.8	Cyber Security Policy	cyber security is reflected in business continuity management.	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	
3.1.4	Cyber Security Roles and Responsibilities	Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization. Additionally, all parties involved in cyber security should understand and take their role and responsibilities.	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	
3.1.4.1	Cyber Security Roles and Responsibilities	The Board of Directors has the ultimate responsibility for cyber security, including:	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.1.a	Cyber Security Roles and Responsibilities	ensuring that sufficient budget for cyber security is allocated;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.1.b	Cyber Security Roles and Responsibilities	approving the cyber security committee charter;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.1.c	Cyber Security Roles and Responsibilities	endorsing (after being approved by the cyber security committee):	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.1.c.1	Cyber Security Roles and Responsibilities	the cyber security governance;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.1.c.2	Cyber Security Roles and Responsibilities	the cyber security 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.	5	
3.1.4.1.c.3	Cyber Security Roles and Responsibilities	the cyber security policy.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2	Cyber Security Roles and Responsibilities	The cyber security committee should be 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.	5	
3.1.4.2.a	Cyber Security Roles and Responsibilities	monitoring, reviewing and communicating the Member Organization's cyber security risk appetite periodically or upon a material change in the risk appetite;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.b	Cyber Security Roles and Responsibilities	reviewing the cyber security strategy to ensure that it supports the Member Organization objectives;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c	Cyber Security Roles and Responsibilities	approving, communicating, supporting and monitoring:	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c.1	Cyber Security Roles and Responsibilities	the cyber security governance;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c.2	Cyber Security Roles and Responsibilities	the cyber security 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.	5	
3.1.4.2.c.3	Cyber Security Roles and Responsibilities	the cyber security policy;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c.4	Cyber Security Roles and Responsibilities	cyber security programs (e.g., awareness program, data classification program, data privacy, data leakage prevention, key cyber security improvements);	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c.5	Cyber Security Roles and Responsibilities	cyber security risk management process;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.2.c.6	Cyber Security Roles and Responsibilities	the key risk indicators (KRIs) and key performance indicators (KPIs) for cyber security.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.3	Cyber Security Roles and Responsibilities	The senior management should be 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.	5	
3.1.4.3.a	Cyber Security Roles and Responsibilities	ensuring that standards, processes and procedures reflect security requirements (if applicable);	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.3.b	Cyber Security Roles and Responsibilities	ensuring that individuals accept and comply with the cyber security policy, supporting standards and procedures when they are issued and updated;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.3.c	Cyber Security Roles and Responsibilities	ensuring that cyber security responsibilities are incorporated in the job descriptions of key positions and cyber security staff.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.4	Cyber Security Roles and Responsibilities	The CISO should be 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).	5	
3.1.4.4.a	Cyber Security Roles and Responsibilities	developing and maintaining:	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	
3.1.4.4.a.1	Cyber Security Roles and Responsibilities	cyber security strategy;	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	
3.1.4.4.a.2	Cyber Security Roles and Responsibilities	cyber security policy;	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	
3.1.4.4.a.3	Cyber Security Roles and Responsibilities	cyber security architecture;	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	
3.1.4.4.a.4	Cyber Security Roles and Responsibilities	cyber security risk management process;	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	
3.1.4.4.b	Cyber Security Roles and Responsibilities	ensuring that detailed security standards and procedures are established, approved and implemented;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.1.4.4.c	Cyber Security Roles and Responsibilities	delivering risk-based cyber security solutions that address people, process and technology;	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	
3.1.4.4.d	Cyber Security Roles and Responsibilities	developing the cyber security staff to deliver cyber security solutions in a business context;	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	
3.1.4.4.e	Cyber Security Roles and Responsibilities	the cyber security activities across the Member Organization, including:	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	
3.1.4.4.e.1	Cyber Security Roles and Responsibilities	monitoring of the cyber security activities (SOC monitoring);	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	
3.1.4.4.e.2	Cyber Security Roles and Responsibilities	monitoring of compliance with cyber security regulations, policies, standards and procedures;	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	
3.1.4.4.e.3	Cyber Security Roles and Responsibilities	overseeing the investigation of cyber security incidents;	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	
3.1.4.4.e.4	Cyber Security Roles and Responsibilities	gathering and analyzing threat intelligence from internal and external sources;	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	
3.1.4.4.e.5	Cyber Security Roles and Responsibilities	performing cyber security reviews;	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	
3.1.4.4.f	Cyber Security Roles and Responsibilities	conducting cyber security risk assessments on the Members Organization's information assets;	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	
3.1.4.4.g	Cyber Security Roles and Responsibilities	proactively supporting other functions on cyber security, including:	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	
3.1.4.4.g.1	Cyber Security Roles and Responsibilities	performing information and system classifications;	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	
3.1.4.4.g.2	Cyber Security Roles and Responsibilities	determining cyber security requirements for important projects;	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	
3.1.4.4.g.3	Cyber Security Roles and Responsibilities	performing cyber security reviews.	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	
3.1.4.4.h	Cyber Security Roles and Responsibilities	defining and conducting the cyber security awareness programs;	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	
3.1.4.4.i	Cyber Security Roles and Responsibilities	measuring and reporting the KRIs and KPIs on:	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	
3.1.4.4.i.1	Cyber Security Roles and Responsibilities	cyber security strategy;	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	
3.1.4.4.i.2	Cyber Security Roles and Responsibilities	cyber security policy compliance;	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	
3.1.4.4.i.3	Cyber Security Roles and Responsibilities	cyber security standards and procedures;	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	
3.1.4.4.i.4	Cyber Security Roles and Responsibilities	cyber security programs (e.g., awareness program, data classification program, key cyber security improvements).	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	
3.1.4.5	Cyber Security Roles and Responsibilities	The internal audit function should be 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.	5	
3.1.4.5.a	Cyber Security Roles and Responsibilities	performing cyber security audits.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
3.1.4.6	Cyber Security Roles and Responsibilities	All Member Organization's staff should be responsible for:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.1.4.6.a	Cyber Security Roles and Responsibilities	complying with cyber security policy, standards and procedures.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.1.5	Cyber Security in Project Management	Cyber security should be addressed in project management and project governance.	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	
3.1.5	Cyber Security in Project Management	Cyber security should be addressed in project management and project governance.	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	
3.1.5.1	Cyber Security in Project Management	Cyber security should be integrated into the Member Organization's project management methodology to ensure that cyber security risks are identified and addressed as part of a project.	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	
3.1.5.1	Cyber Security in Project Management	Cyber security should be integrated into the Member Organization's project management methodology to ensure that cyber security risks are identified and addressed as part of a project.	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	
3.1.5.2	Cyber Security in Project Management	The Member Organization's project management methodology should ensure that:	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	
3.1.5.2.a	Cyber Security in Project Management	cyber security objectives are included in project objectives;	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	
3.1.5.2.b	Cyber Security in Project Management	the cyber security function is part of all phases of the project;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.1.5.2.c	Cyber Security in Project Management	a risk assessment is performed at the start of the project to determine the cyber security risks and to ensure that cyber security requirements are addressed either by the existing cyber security controls (based on cyber security standards) or to be developed;	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	
3.1.5.2.d	Cyber Security in Project Management	cyber security risks are registered in the project-risk register and tracked;	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	
3.1.5.2.e	Cyber Security in Project Management	responsibilities for cyber security are defined and allocated;	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	
3.1.5.2.f	Cyber Security in Project Management	a cyber security review is performed by an independent internal or external party.	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	
3.1.6	Cyber Security Awareness	A cyber security awareness program should be defined and conducted for staff, third parties and customers of the Member Organization.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.1	Cyber Security Awareness	The cyber security awareness programs should be defined, approved and conducted to promote cyber security awareness and to create a positive cyber security culture.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.2	Cyber Security Awareness	A cyber security awareness program should be defined and conducted for:	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.2.a	Cyber Security Awareness	staff of the Member Organization;	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.2.b	Cyber Security Awareness	third parties of the Member Organization;	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.2.c	Cyber Security Awareness	customers of the Member Organization.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.3	Cyber Security Awareness	The cyber security awareness program should target cyber security behaviors by tailoring the program to address the different target groups through multiple channels.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.4	Cyber Security Awareness	The activities of the cyber security awareness program should be conducted periodically and throughout the year.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.5	Cyber Security Awareness	The cyber security awareness program should at a minimum include:	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.5.a	Cyber Security Awareness	an explanation of cyber security measures provided;	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.5.b	Cyber Security Awareness	the roles and responsibilities regarding cyber security;	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.5.c	Cyber Security Awareness	information on relevant emerging cyber security events and cyber threats (e.g., spear-phishing, whaling).	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
3.1.6.6	Cyber Security Awareness	The cyber security awareness program should be evaluated to:	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5	
3.1.6.6.a	Cyber Security Awareness	measure the effectiveness of the awareness activities;	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5	
3.1.6.6.b	Cyber Security Awareness	formulate recommendations to improve the cyber security awareness program.	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5	
3.1.6.7	Cyber Security Awareness	Customer awareness should address for both retail and commercial customers and, at a minimum, include a listing of suggested cyber security mechanisms which customers may consider implementing to mitigate their own risk(s).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
3.1.7	Cyber Security Training	Staff of the Member Organization should be provided with training regarding how to operate the Member Organization's systems securely and to address and apply cyber security controls.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
3.1.7.1	Cyber Security Training	Specialist or security-related skills training should be provided to staff in the Member Organization's relevant functional area categories in line with their job descriptions, including:	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	
3.1.7.1.a	Cyber Security Training	key roles within the organization;	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	
3.1.7.1.b	Cyber Security Training	staff of the cyber security function;	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	
3.1.7.1.c	Cyber Security Training	staff involved in developing and (technically) maintaining 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	
3.1.7.1.d	Cyber Security Training	staff involved in risk assessments.	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	
3.1.7.2	Cyber Security Training	Education should be provided in order to equip staff with the skills and required knowledge to securely operate the Member Organization'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	
3.2	Cyber Security Risk Management and Compliance	See FDE for details.	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.2.1	Cyber Security Risk Management	A cyber security risk management process should be defined, approved and implemented, and should be aligned with the Member Organization's enterprise risk management process.	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	
3.2.1.1-1	Cyber Security Risk Management	The cyber security risk management process should be defined, approved and implemented.	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	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.2-1	Cyber Security Risk Management	The cyber security risk management process should focus on safeguarding the confidentiality, integrity and availability of information assets.	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	There are multiple 3.2.1.2 control numbers, so a number was attached to the end to separate them.
3.2.1.3-1	Cyber Security Risk Management	The cyber security risk management process should be aligned with the existing enterprise risk management process.	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.4-1	Cyber Security Risk Management	The cyber security risk management process should be documented and address:	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	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-1.a	Cyber Security Risk Management	risk identification;	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
3.2.1.4-1.b	Cyber Security Risk Management	risk analysis;	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
3.2.1.4-1.c	Cyber Security Risk Management	risk response;	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
3.2.1.4-1.d	Cyber Security Risk Management	risk monitoring and review.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	5	
3.2.1.4-1.d	Cyber Security Risk Management	risk monitoring and review.	Functional	Intersects With	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	5	
3.2.1.5	Cyber Security Risk Management	The cyber security risk management process should address the Member Organization's information assets, including (but not limited to):	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	
3.2.1.5.a	Cyber Security Risk Management	business processes;	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	
3.2.1.5.b	Cyber Security Risk Management	business applications;	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	
3.2.1.5.c	Cyber Security Risk Management	infrastructure 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	
3.2.1.6	Cyber Security Risk Management	The cyber security risk management process should be initiated:	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	
3.2.1.6.a	Cyber Security Risk Management	at an early stage of the project;	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	
3.2.1.6.b	Cyber Security Risk Management	prior to critical change;	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	
3.2.1.6.c	Cyber Security Risk Management	when outsourcing is being considered;	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	
3.2.1.6.d	Cyber Security Risk Management	when launching new products and technologies.	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	
3.2.1.7	Cyber Security Risk Management	Existing information assets should be periodically subject to cyber security risk assessment based on their classification or risk profile.	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	
3.2.1.8	Cyber Security Risk Management	The cyber security risk management activities should involve:	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	
3.2.1.8.a	Cyber Security Risk Management	business owners;	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	
3.2.1.8.b	Cyber Security Risk Management	IT specialists;	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	
3.2.1.8.c	Cyber Security Risk Management	cyber security specialists;	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	
3.2.1.8.d	Cyber Security Risk Management	key user representatives.	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.2.1.9	Cyber Security Risk Management	The result of the risk assessment should be reported to the relevant business owner (i.e., risk owner) within the Member Organization;	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-04.4	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	5	
3.2.1.10	Cyber Security Risk Management	The relevant business owner (i.e., risk owner) within the Member Organization should accept and endorse the risk assessment results.	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	
3.2.1.10	Cyber Security Risk Management	The relevant business owner (i.e., risk owner) within the Member Organization should accept and endorse the risk assessment results.	Functional	Intersects With	Executive Leadership Approval For Managing Material Risk	RSK-13	Mechanisms exist to obtain executive leadership approval for risk management decisions involving material risk.	3	
3.2.1.11	Cyber Security Risk Management	The Member Organization's cyber security risk appetite and risk tolerance should be clearly defined and formally approved.	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
3.2.1.11	Cyber Security Risk Management	The Member Organization's cyber security risk appetite and risk tolerance should be clearly defined and formally approved.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
3.2.1.1-2	Cyber Security Risk Identification	Cyber security risk identification should be performed and should include the Member Organization's relevant assets, threats, existing controls and vulnerabilities.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.1-2.1	Cyber Security Risk Identification	Cyber security risk identification should be performed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.1-2.2	Cyber Security Risk Identification	Identified cyber security risks should be documented (in a central register).	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	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.1-2.2	Cyber Security Risk Identification	Identified cyber security risks should be documented (in a central register).	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.1-2.3	Cyber Security Risk Identification	Cyber security risk identification should address relevant information assets, threats, vulnerabilities and the key existing cyber security controls.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	There are multiple 3.2.1.1 control numbers, so a number was attached to the end to separate them.
3.2.1.2-2	Cyber Security Risk Analysis	A cyber security risk analysis should be conducted based on the likelihood that the identified cyber security risks will occur and their resulting impact.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	There are multiple 3.2.1.2 control numbers, so a number was attached to the end to separate them.
3.2.1.2-2.1	Cyber Security Risk Analysis	A cyber security risk analysis should be performed.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	There are multiple 3.2.1.2 control numbers, so a number was attached to the end to separate them.
3.2.1.2-2.2	Cyber Security Risk Analysis	The cyber security risk analysis should address the level of potential business impact and likelihood of cyber security threat events materializing.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	There are multiple 3.2.1.2 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2	Cyber Security Risk Response	The cyber security risks of a Member Organization should be treated.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.1	Cyber Security Risk Response	The relevant determined cyber security risks should be treated according to the Member Organization's risk appetite and cyber security requirements.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.2	Cyber Security Risk Response	Cyber security risk response should ensure that the list of risk treatment options are documented (i.e., accepting, avoiding, transferring or mitigating risks by applying cyber security controls).	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.3	Cyber Security Risk Response	Accepting cyber security risks should include:	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.3.a	Cyber Security Risk Response	the consideration of predefined limits for levels of cyber security risk;	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.3.b	Cyber Security Risk Response	the approval and sign-off by the business owner, ensuring that:	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.3.b.1	Cyber Security Risk Response	the accepted cyber security risk is within the risk appetite and is reported to the cyber security committee;	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.3.b.2	Cyber Security Risk Response	the accepted cyber security risk does not contradict SAMA regulations.	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.4	Cyber Security Risk Response	Avoiding cyber security risks should involve a decision by a business owner to cancel or postpone a particular activity or project that introduces an unacceptable cyber security risk.	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.2.1.3-2.5	Cyber Security Risk Response	Transferring or sharing the cyber security risks should:	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.5.a	Cyber Security Risk Response	involve sharing the cyber security risks with relevant (internal or external) providers;	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.5.b	Cyber Security Risk Response	be accepted by the receiving (internal or external) provider(s);	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.5.c	Cyber Security Risk Response	eventually lead to the actual transferring or sharing of the cyber security risk.	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	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6	Cyber Security Risk Response	Applying cyber security controls to mitigate cyber security risks should include:	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.a	Cyber Security Risk Response	identifying appropriate cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.b	Cyber Security Risk Response	evaluating the strengths and weaknesses of the cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.b.1	Cyber Security Risk Response	assessing the cost of implementing the cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.b.2	Cyber Security Risk Response	assessing the feasibility of implementing the cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.b.3	Cyber Security Risk Response	reviewing relevant compliance requirements for the cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.c	Cyber Security Risk Response	selecting cyber security controls;	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.6.d	Cyber Security Risk Response	identifying, documenting and obtaining sign-off for any residual risk by the business owner.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.3-2.7	Cyber Security Risk Response	Cyber security risk treatment actions should be documented in a risk treatment plan.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.3 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2	Cyber Risk Monitoring and Review	The progress cyber security risk treatment should be monitored and the effectiveness of revised or newly implemented cyber security controls should be reviewed.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2.1	Cyber Risk Monitoring and Review	The cyber security treatment should be monitored, including:	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2.1.a	Cyber Risk Monitoring and Review	tracking progress in accordance to treatment plan;	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2.1.b	Cyber Risk Monitoring and Review	the selected and agreed cyber security controls are being implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2.2	Cyber Risk Monitoring and Review	The design and effectiveness of the revised or newly implemented cyber security controls should be reviewed.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.1.4-2.2	Cyber Risk Monitoring and Review	The design and effectiveness of the revised or newly implemented cyber security controls should be reviewed.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	3	There are multiple 3.2.1.4 control numbers, so a number was attached to the end to separate them.
3.2.2	Regulatory Compliance	A process should be established by the Member Organization to identify, communicate and comply with the cyber security implications of relevant regulations.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.2.2.1	Regulatory Compliance	A process should be established for ensuring compliance with relevant regulatory requirements affecting cyber security across the Member Organization. The process of ensuring compliance should:	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.2.2.1.a	Regulatory Compliance	be performed periodically or when new regulatory requirements become effective;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.2.2.1.b	Regulatory Compliance	involve representatives from key areas of the Member Organization;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.2.2.1.c	Regulatory Compliance	result in the update of cyber security policy, standards and procedures to accommodate any necessary changes (if applicable).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
3.2.3	Compliance with (inter)national industry standards	The Member Organization should comply with mandatory (inter)national industry standards.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.2.3.1	Compliance with (inter)national industry standards	The Member Organization should comply with:	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	5	
3.2.3.1.a	Compliance with (inter)national industry standards	Payment Card Industry Data Security Standard (PCI-DSS);	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	5	
3.2.3.1.b	Compliance with (inter)national industry standards	EMV (Europay, MasterCard and Visa) technical standard;	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	5	
3.2.3.1.c	Compliance with (inter)national industry standards	SWIFT Customer Security Controls Framework – March 2017.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	5	
3.2.4	Cyber Security Review	The cyber security status of the Member Organization's information assets should be subject to periodic cyber security review.	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	
3.2.4.1	Cyber Security Review	Cyber security reviews should be periodically performed for critical information assets.	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	
3.2.4.2	Cyber Security Review	Customer and internet facing services should be subject to annual review and penetration tests.	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	
3.2.4.3	Cyber Security Review	Details of cyber security review performed should be recorded, including the results of review, issues identified and recommended actions.	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	
3.2.4.4	Cyber Security Review	The results of cyber security review should be reported to business owner.	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	
3.2.4.5	Cyber Security Review	Cyber security review should be subject to follow-up reviews to check that:	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	
3.2.4.5.a	Cyber Security Review	all identified issues have been addressed;	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	
3.2.4.5.b	Cyber Security Review	critical risks have been treated effectively;	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	
3.2.4.5.c	Cyber Security Review	all agreed actions are being managed on an ongoing basis.	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	
3.2.5	Cyber Security Audits	The cyber security status of the Member Organization's information assets should be subject to thorough, independent and regular cyber security audits performed in accordance with generally accepted auditing standards and SAMA cyber security framework.	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	
3.2.5.1	Cyber Security Audits	Cyber security audits should be performed independently and according to generally accepted auditing standards and SAMA cyber security framework.	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	
3.2.5.2	Cyber Security Audits	Cyber security audits should be performed according to the Member Organization's audit manual and audit plan.	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	
3.3	Cyber Security Operations and Technology	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.1	Cyber Security Operations and Technology	The Member Organization should incorporate cyber security requirements into human resources processes.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
3.3.1.1	Cyber Security Operations and Technology	The human resources process should define, approve and implement cyber security requirements.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
3.3.1.2	Cyber Security Operations and Technology	The effectiveness of the human resources process should be monitored, measured and periodically evaluated.	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	
3.3.1.3	Cyber Security Operations and Technology	The human resource process should include:	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
3.3.1.3.a	Cyber Security Operations and Technology	cyber security responsibilities and non-disclosure clauses within staff agreements (during and after the employment);	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.1.3.a	Cyber Security Operations and Technology	cyber security responsibilities and non-disclosure clauses within staff agreements (during and after the employment);	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
3.3.1.3.b	Cyber Security Operations and Technology	staff should receive cyber security awareness at the start and during their employment;	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5	
3.3.1.3.b	Cyber Security Operations and Technology	staff should receive cyber security awareness at the start and during their employment;	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5	
3.3.1.3.b	Cyber Security Operations and Technology	staff should receive cyber security awareness at the start and during their employment;	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
3.3.1.3.c	Cyber Security Operations and Technology	when disciplinary actions will be applicable;	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
3.3.1.3.d	Cyber Security Operations and Technology	screening and background check;	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
3.3.1.3.d	Cyber Security Operations and Technology	screening and background check;	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	
3.3.1.3.e	Cyber Security Operations and Technology	post-employment cyber security activities, such as:	Functional	Intersects With	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive and/or regulated data.	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.1.3.e.1	Cyber Security Operations and Technology	revoking access rights;	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
3.3.1.3.e.2	Cyber Security Operations and Technology	returning information assets assigned (e.g., access badge, tokens, mobile devices, all electronic and physical information).	Functional	Intersects With	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	5	
3.3.1.3.e.2	Cyber Security Operations and Technology	returning information assets assigned (e.g., access badge, tokens, mobile devices, all electronic and physical information).	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
3.3.2	Physical Security	The Member Organization should ensure all facilities which host information assets are physically protected against intentional and unintentional security events.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.3.2.1	Physical Security	The physical security process should be defined, approved and implemented.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.3.2.2	Physical Security	The effectiveness of the physical security process should be monitored, measured and periodically evaluated.	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	
3.3.2.3	Physical Security	The physical security process should include (but not limited to):	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.3.2.3.a	Physical Security	physical entry controls (including visitor security);	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.3.2.3.b	Physical Security	monitoring and surveillance (e.g., CCTV, ATMs GPS tracking, sensitivity sensors);	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
3.3.2.3.c	Physical Security	protection of data centers and data rooms;	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
3.3.2.3.d	Physical Security	environmental protection;	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
3.3.2.3.e	Physical Security	protection of information assets during lifecycle (including transport and secure disposal, avoiding unauthorized access and (un)intended data leakage.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.3.2.3.e	Physical Security	protection of information assets during lifecycle (including transport and secure disposal, avoiding unauthorized access and (un)intended data leakage.	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	
3.3.2.3.e	Physical Security	protection of information assets during lifecycle (including transport and secure disposal, avoiding unauthorized access and (un)intended data leakage.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
3.3.3	Asset Management	The Member Organization should define, approve, implement, communicate and monitor an asset management process, which supports an accurate, up-to-date and unified asset register.	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	
3.3.3.1	Asset Management	The asset management process should be defined, approved and implemented.	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	
3.3.3.2	Asset Management	The effectiveness of the asset management process should be monitored, measured and periodically evaluated.	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	
3.3.3.3	Asset Management	The asset management process should include:	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	
3.3.3.3	Asset Management	The asset management process should include:	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.3.3.a	Asset Management	a unified register;	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.3.3.b	Asset Management	ownership and custodianship of information assets;	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.3.3.c	Asset Management	the reference to relevant other processes, depending on asset management;	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.3.3.d	Asset Management	information asset classification, labeling and handling;	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.3.3.e	Asset Management	the discovery of new information assets.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.3.4	Cyber Security Architecture	The Member Organization should define, follow and review the cyber security architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities.	Functional	Intersects With	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	5	
3.3.4.1	Cyber Security Architecture	The cyber security architecture should be defined, approved and implemented.	Functional	Intersects With	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	5	
3.3.4.2	Cyber Security Architecture	The compliance with the cyber security architecture should be monitored.	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	
3.3.4.3	Cyber Security Architecture	The cyber security architecture should include:	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	
3.3.4.3.a	Cyber Security Architecture	a strategic outline of cyber security capabilities and controls based on the business requirements;	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.3.4.3.b	Cyber Security Architecture	approval of the defined cyber security architecture;	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	
3.3.4.3.c	Cyber Security Architecture	the requirement of having qualified cyber security architects;	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	
3.3.4.3.d	Cyber Security Architecture	design principles for developing cyber security controls and applying cyber security requirements (i.e., the security-by-design principle);	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	
3.3.4.3.e	Cyber Security Architecture	periodic review of the cyber security architecture.	Functional	Subset Of	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	10	
3.3.5	Identity and Access Management	The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.	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	
3.3.5.1	Identity and Access Management	The identity and access management policy, including the responsibilities and accountabilities, should be defined, approved and implemented.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
3.3.5.1	Identity and Access Management	The identity and access management policy, including the responsibilities and accountabilities, should be defined, approved and implemented.	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	
3.3.5.2	Identity and Access Management	The compliance with the identity and access policy should be monitored.	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	
3.3.5.3	Identity and Access Management	The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.	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	
3.3.5.4	Identity and Access Management	The identity and access management policy should include:	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	
3.3.5.4.a	Identity and Access Management	business requirements for access control (i.e., need-to-have and need-to-know);	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	
3.3.5.4.b	Identity and Access Management	user access management (e.g., joiners, movers, leavers):	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	
3.3.5.4.b.1	Identity and Access Management	all identified user types should be covered (i.e., internal staff, third parties);	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	
3.3.5.4.b.2	Identity and Access Management	changes of job status or job positions for internal staff (e.g. joiner, mover and leaver) should be instigated by the human resources department;	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	
3.3.5.4.b.3	Identity and Access Management	changes for external staff or third parties should be instigated by the appointed accountable party;	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	
3.3.5.4.b.4	Identity and Access Management	user access requests are formally approved in accordance with business and compliance requirements (i.e., need-to-have and need-to-know to avoid unauthorized access and (un)intended data leakage));	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	
3.3.5.4.b.5	Identity and Access Management	changes in access rights should be processed in a timely manner;	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	
3.3.5.4.b.6	Identity and Access Management	periodically user access rights and profiles should be reviewed;	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	
3.3.5.4.b.7	Identity and Access Management	an audit trail of submitted, approved and processed user access requests and revocation requests should be established;	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	
3.3.5.4.c	Identity and Access Management	user access management should be supported by automation;	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	
3.3.5.4.d	Identity and Access Management	centralization of the identity and access management function;	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	
3.3.5.4.e	Identity and Access Management	multi-factor authentication for sensitive and critical systems and profiles;	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	
3.3.5.4.f	Identity and Access Management	privileged and remote access management, which should address:	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	
3.3.5.4.f.1	Identity and Access Management	the allocation and restricted use of privileged and remote access, specifying:	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	
3.3.5.4.f.1.a	Identity and Access Management	multi-factor authentication should be used for all remote access;	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	
3.3.5.4.f.1.b	Identity and Access Management	multi-factor authentication should be used for privilege access on critical systems based on a risk assessment;	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	
3.3.5.4.f.2	Identity and Access Management	the periodic review of users with privileged and remote accounts;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.5.4.f.3	Identity and Access Management	individual accountability;	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	
3.3.5.4.f.4	Identity and Access Management	the use of non-personal privileged accounts, including:	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	
3.3.5.4.f.4.a	Identity and Access Management	limitation and monitoring;	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	
3.3.5.4.f.4.b	Identity and Access Management	confidentiality of passwords;	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	
3.3.5.4.f.4.c	Identity and Access Management	cchanging passwords frequently and at the end of each session.	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	
3.3.6	Application Security	The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated.	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	
3.3.6.1	Application Security	The application cyber security standards should be defined, approved and implemented.	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	
3.3.6.2	Application Security	The compliance with the application security standards should be monitored.	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	
3.3.6.3	Application Security	The effectiveness of the application cyber security controls should be measured and periodically evaluated.	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	
3.3.6.4	Application Security	Application development should follow the approved secure system development life cycle methodology (SDLC).	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5	Application Security	The application security standard should include:	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.a	Application Security	secure coding standards;	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.b	Application Security	the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], identity and access management);	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.c	Application Security	the segregation of duties within the application (supported with a documented authorization matrix);	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.d	Application Security	the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage);	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.e	Application Security	vulnerability and patch management;	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.f	Application Security	back-up and recovery procedures;	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.6.5.g	Application Security	periodic cyber security compliance review.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3.7	Change Management	The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
3.3.7.1	Change Management	The change management process should be defined, approved and implemented.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
3.3.7.2	Change Management	The compliance with the change management process should be monitored.	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	
3.3.7.3	Change Management	The effectiveness of the cyber security controls within the change management process should be measured and periodically evaluated.	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	
3.3.7.4	Change Management	The change management process should include:	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
3.3.7.4.a	Change Management	cyber security requirements for controlling changes to information assets, such as assessing the impact of requested changes, classification of changes and the review of changes;	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	
3.3.7.4.b	Change Management	security testing, which should (if applicable) include:	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	
3.3.7.4.b.1	Change Management	penetration testing;	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	
3.3.7.4.b.2	Change Management	code review if applications are developed internally;	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	

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
3.3.7.4.b.3	Change Management	code review of externally developed applications and if the source code is available	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	
3.3.7.4.b.4	Change Management	a code review report (or equivalent, such as an independent assurance statement) in case the source code cannot be provided;	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	
3.3.7.4.c	Change Management	approval of changes by the business owner;	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
3.3.7.4.d	Change Management	approval from the cyber security function before submitting to Change Advisory Board (CAB);	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
3.3.7.4.e	Change Management	approval by CAB;	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
3.3.7.4.f	Change Management	post-implementation review of the related cyber security controls;	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
3.3.7.4.g	Change Management	development, testing and implementation are segregated for both the (technical) environment and involved individuals;	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	
3.3.7.4.h	Change Management	the procedure for emergency changes and fixes;	Functional	Intersects With	Emergency Changes	CHG-07	Mechanisms exist to govern change management procedures for "emergency" changes.	5	
3.3.7.4.i	Change Management	fall-back and roll-back procedures.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
3.3.8	Infrastructure Security	The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated.	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	
3.3.8.1	Infrastructure Security	The infrastructure security standards should be defined, approved and implemented.	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	
3.3.8.2	Infrastructure Security	The compliance with the infrastructure security standards should be monitored.	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	
3.3.8.3	Infrastructure Security	The effectiveness of the infrastructure cyber security controls should be measured and periodically evaluated.	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	
3.3.8.4	Infrastructure Security	The infrastructure security standards should cover all instances of infrastructure available in the main datacenter(s), the disaster recovery data site(s) and office spaces.	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	
3.3.8.5	Infrastructure Security	The infrastructure security standards should cover all instances of infrastructure (e.g., operating systems, servers, virtual machines, firewalls, network devices, IDS, IPS, wireless network, gateway servers, proxy servers, email gateways, external connections, databases, file-shares, workstations, laptops, tablets, mobile devices, PBX).	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	
3.3.8.6	Infrastructure Security	The infrastructure security standard should include:	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	
3.3.8.6.a	Infrastructure Security	the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance);	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	
3.3.8.6.b	Infrastructure Security	the segregation of duties within the infrastructure component (supported with a documented authorization matrix);	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	
3.3.8.6.c	Infrastructure Security	the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage);	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	
3.3.8.6.d	Infrastructure Security	the use of approved software and secure protocols;	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	
3.3.8.6.e	Infrastructure Security	segmentation of networks;	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	
3.3.8.6.f	Infrastructure Security	malicious code/software and virus protection (and applying application whitelisting and APT protection);	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	
3.3.8.6.g	Infrastructure Security	vulnerability and patch management;	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	
3.3.8.6.h	Infrastructure Security	DDOS protection (where applicable); this should include:	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	
3.3.8.6.h.1	Infrastructure Security	the use of scrubbing services;	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	
3.3.8.6.h.2	Infrastructure Security	specification of the bandwidth agreed;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.8.6.h.3	Infrastructure Security	24x7 monitoring by Security Operating Center (SOC), Service Provider (SP) and scrubbing provider;	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	
3.3.8.6.h.4	Infrastructure Security	testing of DDOS scrubbing (minimum twice a year);	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	
3.3.8.6.h.5	Infrastructure Security	DDOS services should be implemented for the main datacenter(s) as well as the disaster recovery site(s);	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	
3.3.8.6.i	Infrastructure Security	back-up and recovery procedures;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
3.3.8.6.j	Infrastructure Security	periodic cyber security compliance review.	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	
3.3.9	Cryptography	The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented.	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	
3.3.9.1	Cryptography	A cryptographic security standard should be defined, approved and implemented.	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	
3.3.9.2	Cryptography	The compliance with the cryptographic security standard should be monitored.	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	
3.3.9.3	Cryptography	The effectiveness of the cryptographic security controls should be measured and periodically evaluated.	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	
3.3.9.4	Cryptography	The cryptographic security standard should include:	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
3.3.9.4.a	Cryptography	an overview of the approved cryptographic solutions and relevant restrictions (e.g., technically, legally);	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
3.3.9.4.b	Cryptography	the circumstances when the approved cryptographic solutions should be applied;	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
3.3.9.4.c	Cryptography	the management of encryption keys, including lifecycle management, archiving and recovery.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
3.3.10	Bring Your Own Device (BYOD)	When the Member Organization allows the use of personal devices (e.g., smartphones, tablets, laptops) for business purposes, the use should be supported by a defined, approved and implemented cyber security standard, additional staff agreements and a cyber security awareness training.	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	
3.3.10	Bring Your Own Device (BYOD)	When the Member Organization allows the use of personal devices (e.g., smartphones, tablets, laptops) for business purposes, the use should be supported by a defined, approved and implemented cyber security standard, additional staff agreements and a cyber security awareness training.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
3.3.10.1	Bring Your Own Device (BYOD)	The BYOD cyber security standard should be defined, approved and implemented.	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	
3.3.10.2	Bring Your Own Device (BYOD)	The compliance with the BYOD cyber security standard should be monitored.	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	
3.3.10.3	Bring Your Own Device (BYOD)	The effectiveness of the BYOD cyber security controls should be measured and periodically evaluated.	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	
3.3.10.4	Bring Your Own Device (BYOD)	The BYOD standard should include:	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	
3.3.10.4.a	Bring Your Own Device (BYOD)	responsibilities of the user (including awareness training);	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	
3.3.10.4.b	Bring Your Own Device (BYOD)	information regarding the restrictions and consequences for staff when the Member Organization implements cyber security controls on their personal devices; for example when using modified devices (jailbreaking), terminating the employment or in case of loss or theft of the personal device;	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	
3.3.10.4.c	Bring Your Own Device (BYOD)	the isolation of business information from personal information (e.g., containerization);	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	
3.3.10.4.d	Bring Your Own Device (BYOD)	the regulation of corporate mobile applications or approved "public" mobile applications;	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	
3.3.10.4.e	Bring Your Own Device (BYOD)	the use of mobile device management (MDM); applying access controls to the device and business container and encryption mechanisms on the personal device (to ensure secure transmission and storage).	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	
3.3.11	Secure Disposal of Information Assets	The information assets of the Member Organization should be securely disposed when the information assets are no longer required.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.3.11.1	Secure Disposal of Information Assets	The secure disposal standard and procedure should be defined, approved and implemented.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.3.11.2	Secure Disposal of Information Assets	The compliance with the secure disposal standard and procedure should be monitored.	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	
3.3.11.3	Secure Disposal of Information Assets	The effectiveness of the secure disposal cyber security controls should be measured and periodically evaluated.	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	
3.3.11.4	Secure Disposal of Information Assets	Information assets should be disposed in accordance with legal and regulatory requirements, when no longer required (i.e. meeting data privacy regulations to avoid unauthorized access and avoid (un)intended data leakage).	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.3.11.5	Secure Disposal of Information Assets	Sensitive information should be destroyed using techniques to make the information non-retrievable (e.g., secure erase, secure wiping, incineration, double crosscut, shredding).	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.11.6	Secure Disposal of Information Assets	The Member Organization should ensure that third party service providers used for secure disposal, transport and storage comply with the secure disposal standard and procedure and the effectiveness is periodically measured and evaluated.	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	
3.3.12	Payment Systems	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13	Electronic Banking Services	The Member Organization should define, approve, implement and monitor a cyber security standard for electronic banking services. The effectiveness of this standard should be measured and periodically evaluated.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.1	Electronic Banking Services	The cyber security standards for electronic banking services should be defined, approved and implemented.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.2	Electronic Banking Services	The compliance with cyber security standards for electronic banking services should be monitored.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.3	Electronic Banking Services	The effectiveness of the cyber security standard for electronic banking services should be measured and periodically evaluated.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4	Electronic Banking Services	Electronic banking services security standard should cover:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.a	Electronic Banking Services	use of brand protection measures to protect online services including social media.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b	Electronic Banking Services	online, mobile and phone banking:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.1	Electronic Banking Services	use of official application stores and websites (applicable for online and mobile banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.2	Electronic Banking Services	use of detection measures and take-down of malicious apps and websites (applicable for online and mobile banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.3	Electronic Banking Services	use of sandboxing (applicable for online and mobile banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.4	Electronic Banking Services	use of non-caching techniques (applicable for online and mobile banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.5	Electronic Banking Services	use of communication techniques to avoid 'man-in-the-middle'-attacks (applicable for online and mobile banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6	Electronic Banking Services	use of multi-factor authentication mechanisms:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.a	Electronic Banking Services	multi-factor authentication should be used during the registration process for the customer in order to use of electronic banking services;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.b	Electronic Banking Services	multi-factor authentication should be implemented for all electronic banking services available to customers;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.c	Electronic Banking Services	the use of hard and soft tokens should be password protected;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.d	Electronic Banking Services	revoking the access of customers after 3 successive incorrect passwords or invalid PINs;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.e	Electronic Banking Services	the process for changing the customer mobile number should only be done from either a branch or ATM;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.f	Electronic Banking Services	the processes for requesting and activating of the multi-factor authentication should be done through different delivery channels;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g	Electronic Banking Services	multi-factor authentication should be implemented for the following processes:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g.1	Electronic Banking Services	sign-on;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g.2	Electronic Banking Services	adding or modifying beneficiaries;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g.3	Electronic Banking Services	adding utility and government payment services;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g.4	Electronic Banking Services	high-risk transactions (when it exceeds predefined limits);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.6.g.5	Electronic Banking Services	password reset;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.7	Electronic Banking Services	the processes for adding and activating beneficiaries should be done through different delivery channels (applicable for mobile and online banking);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.8	Electronic Banking Services	high availability of the electronic banking services should be ensured;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.9	Electronic Banking Services	scheduled downtime of the electronic banking services should be timely communicated to SAMA and customers;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.10	Electronic Banking Services	contractual agreements between the Member Organization and the customer addressing the roles, responsibilities and liabilities for both the Member Organization and the customers;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.b.11	Electronic Banking Services	obtaining approval of SAMA before launching a new electronic banking service.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.c	Electronic Banking Services	ATMs and POSs:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.c.1	Electronic Banking Services	prevention and detection of exploiting the ATM/POS application and infrastructure vulnerabilities (e.g., cables, (USB)-ports, rebooting);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.c.2	Electronic Banking Services	cyber security measures, such as hardening of operating systems, malware protection, privacy screens, masking of passwords or account numbers (e.g., screen and receipt), geo-blocking (e.g., disable cards per default for outside GCC countries, disable magnetic strip transactions), video monitoring (CCTV), revoking cards after 3 successive invalid PINs, anti-skimming solutions (hardware/software), and PIN-pad protection;	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	
3.3.13.4.c.3	Electronic Banking Services	remote stopping of ATMs in case of malicious activities.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d	Electronic Banking Services	SMS instant notification services:	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d.1	Electronic Banking Services	SMS messages should not contain sensitive data (e.g., account balance - except for credit cards);	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d.2	Electronic Banking Services	SMS alert should be sent to both mobile numbers (old and new) when the customer's mobile number has been changed;	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d.3	Electronic Banking Services	SMS notification should be sent to the customer's mobile number when requesting a new multifactor authentication mechanism.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d.4	Electronic Banking Services	SMS notification should be sent to the customer's mobile number for all retail and personal financial transactions.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.13.4.d.5	Electronic Banking Services	SMS notification should be sent to the customer's mobile number when beneficiaries are added, modified and activated.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.14	Cyber Security Event Management	The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
3.3.14.1	Cyber Security Event Management	The security event management process should be defined, approved and implemented.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
3.3.14.2	Cyber Security Event Management	The effectiveness of the cyber security controls within the security event management process should be measured and periodically evaluated.	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	
3.3.14.3	Cyber Security Event Management	To support this process a security event monitoring standard should be defined, approved and implemented.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
3.3.14.3.a	Cyber Security Event Management	the standard should address for all information assets the mandatory events which should be monitored, based on the classification or risk profile of the information asset.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
3.3.14.4	Cyber Security Event Management	The security event management process should include requirements for:	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.a	Cyber Security Event Management	the establishment of a designated team responsible for security monitoring (i.e., Security Operations Center (SOC));	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring 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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.14.4.b	Cyber Security Event Management	skilled and (continuously) trained staff;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.c	Cyber Security Event Management	a restricted area to facilitate SOC activities and workspaces;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.d	Cyber Security Event Management	resources required continuous security event monitoring activities (24x7);	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.e	Cyber Security Event Management	detection and handling of malicious code and software;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.f	Cyber Security Event Management	detection and handling of security or suspicious events and anomalies;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.g	Cyber Security Event Management	deployment of security network packet analysis solution;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.3.14.4.h	Cyber Security Event Management	adequately protected logs;	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.14.4.i	Cyber Security Event Management	periodic compliance monitoring of applications and infrastructure cyber security standards	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	
3.3.14.4.j	Cyber Security Event Management	automated and centralized analysis of security loggings and correlation of event or patterns (i.e., Security Information and Event Management (SIEM));	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	
3.3.14.4.k	Cyber Security Event Management	reporting of cyber security incidents;	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	
3.3.14.4.l	Cyber Security Event Management	independent periodic testing of the effectiveness of the security operations center (e.g., red-teaming).	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	
3.3.15	Cyber Security Incident Management	The Member Organization should define, approve and implement a cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated.	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	
3.3.15.1	Cyber Security Incident Management	The cyber security incident management process should be defined, approved, implemented and aligned with the enterprise incident management process.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
3.3.15.2	Cyber Security Incident Management	The effectiveness of the cyber security controls within the cyber security incident management process should be measured and periodically evaluated.	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	
3.3.15.3	Cyber Security Incident Management	The standard should address the mandatory and suspicious security events which should be responded to.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4	Cyber Security Incident Management	The security incident management process should include requirements for:	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.a	Cyber Security Incident Management	the establishment of a designated team responsible for security incident management;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.b	Cyber Security Incident Management	skilled and (continuously) trained staff;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.c	Cyber Security Incident Management	sufficient capacity available of certified forensic staff for handling major incidents (e.g., internal staff or contracting an external forensic team);	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.d	Cyber Security Incident Management	a restricted area to facilitate the computer emergency response team (CERT) workspaces;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.e	Cyber Security Incident Management	the classification of cyber security incidents;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.f	Cyber Security Incident Management	the timely handling of cyber security incidents, recording and monitoring progress;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.g	Cyber Security Incident Management	the protection of relevant evidence and loggings;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.h	Cyber Security Incident Management	post-incident activities, such as forensics, root-cause analysis of the incidents;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.4.i	Cyber Security Incident Management	reporting of suggested improvements to the CISO and the Committee;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	

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
3.3.15.4.j	Cyber Security Incident Management	establish a cyber security incident repository.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.15.5	Cyber Security Incident Management	The Member Organization should inform 'SAMA IT Risk Supervision' immediately when a medium or high classified security incident has occurred and identified.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.15.6	Cyber Security Incident Management	The Member Organization should obtain 'no objection' from 'SAMA IT Risk Supervision' before any media interaction related to the incident.	Functional	No Relationship	N/A	N/A	N/A	0	
3.3.15.7	Cyber Security Incident Management	The Member Organization should submit a formal incident report 'SAMA IT Risk Supervision' after resuming operations, including the following incident details:	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.a	Cyber Security Incident Management	title of incident;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.b	Cyber Security Incident Management	classification of the incident (medium or high);	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.c	Cyber Security Incident Management	date and time of incident occurred;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.d	Cyber Security Incident Management	date and time of incident detected;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.e	Cyber Security Incident Management	information assets involved;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.f	Cyber Security Incident Management	(technical) details of the incident;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.g	Cyber Security Incident Management	root-cause analysis;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.h	Cyber Security Incident Management	corrective activities performed and planned;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.i	Cyber Security Incident Management	description of impact (e.g., loss of data, disruption of services, unauthorized modification of data, (un)intended data leakage, number of customers impacted);	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.j	Cyber Security Incident Management	total estimated cost of incident;	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.15.7.k	Cyber Security Incident Management	estimated cost of corrective actions.	Functional	Intersects With	Serious Incident Reporting	IRO-10.5	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
3.3.16	Threat Management	The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated.	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	
3.3.16.1	Threat Management	The threat intelligence management process should be defined, approved and implemented.	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	
3.3.16.2	Threat Management	The effectiveness of the threat intelligence management process should be measured and periodically evaluated.	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	
3.3.16.3	Threat Management	The threat intelligence management process should include:	Functional	Subset Of	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.	10	
3.3.16.3.a	Threat Management	the use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tooling, Security Information and Event Monitoring (SIEM), support functions (e.g., Legal, Audit, IT Helpdesk, Forensics, Fraud Management, Risk Management, Compliance);	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	
3.3.16.3.b	Threat Management	the use of reliable and relevant external sources, such as SAMA, government agencies, security forums, (security) vendors, security organizations and specialist notification services;	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	
3.3.16.3.c	Threat Management	a defined methodology to analyze the threat information periodically;	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	

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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.3.16.3.d	Threat Management	the relevant details on identified or collected threats, such as modus operandi, actors, motivation and type of threats;	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	
3.3.16.3.e	Threat Management	the relevance of the derived intelligence and the action-ability for follow-up (for e.g., SOC, Risk Management);	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	
3.3.16.3.f	Threat Management	sharing the relevant intelligence with the relevant stakeholders (e.g., SAMA, BCIS members).	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	
3.3.17	Vulnerability Management	The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
3.3.17.1	Vulnerability Management	The vulnerability management process should be defined, approved and implemented.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
3.3.17.2	Vulnerability Management	The effectiveness of the vulnerability management process should be measured and periodically evaluated.	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	
3.3.17.3	Vulnerability Management	The vulnerability management process should include:	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.a	Vulnerability Management	all information assets;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.b	Vulnerability Management	frequency of performing the vulnerability scan (risk-based);	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.c	Vulnerability Management	classification of vulnerabilities;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.d	Vulnerability Management	defined timelines to mitigate (per classification);	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.e	Vulnerability Management	prioritization for classified information assets;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.17.3.f	Vulnerability Management	patch management and method of deployment.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.4	Third Party Cyber Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.4.1	Contract and Vendor Management	The Member Organization should define, approve, implement and monitor the required cyber security controls within the contract and vendor management processes.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
3.4.1.1	Contract and Vendor Management	The cyber security requirements should be defined, approved, implemented and communicated within the contract and vendor management processes.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
3.4.1.2	Contract and Vendor Management	The compliance with contract and vendor management process should be monitored.	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	
3.4.1.3	Contract and Vendor Management	The effectiveness of the cyber security controls within the contract and vendor management process should be measured and periodically evaluated.	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	
3.4.1.4	Contract and Vendor Management	These contract and vendor management processes should cover:	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
3.4.1.4.a	Contract and Vendor Management	whether the involvement of the cyber security function is actively required (e.g., in case of due diligence);	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
3.4.1.4.b	Contract and Vendor Management	the baseline cyber security requirements which should be applied in all cases;	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).	5	
3.4.1.4.c	Contract and Vendor Management	the right to periodically perform cyber security reviews and audits.	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).	5	
3.4.1.5	Contract and Vendor Management	The contract management process should cover requirements for:	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).	5	
3.4.1.5.a	Contract and Vendor Management	executing a cyber security risk assessment as part of the procurement process;	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).	5	
3.4.1.5.b	Contract and Vendor Management	defining the specific cyber security requirements as part of the tender process;	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).	5	
3.4.1.5.c	Contract and Vendor Management	evaluating the replies of potential vendors on the defined cyber security requirements;	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).	5	
3.4.1.5.d	Contract and Vendor Management	testing of the agreed cyber security requirements (risk-based);	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).	5	
3.4.1.5.e	Contract and Vendor Management	defining the communication or escalation process in case of cyber security incidents;	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).	5	
3.4.1.5.f	Contract and Vendor Management	ensuring cyber security requirements are defined for exiting, terminating or renewing the contract (including escrow agreements if applicable);	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).	5	
3.4.1.5.g	Contract and Vendor Management	defining a mutual confidentiality agreement.	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).	5	
3.4.1.6	Contract and Vendor Management	The vendor management process (i.e., service level management) should cover requirements for:	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
3.4.1.6.a	Contract and Vendor Management	periodic reporting, reviewing and evaluating the contractually agreed cyber security requirements (in SLAs).	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
3.4.2	Outsourcing	The Member Organization should define, implement and monitor the required cyber security controls within outsourcing policy and outsourcing process. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.	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	
3.4.2.1	Outsourcing	The cyber security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within Member Organization.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.4.2.2	Outsourcing	The cyber security requirements regarding the outsourcing policy and process should be measured and periodically evaluated.	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	
3.4.2.3	Outsourcing	The outsourcing process should include:	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
3.4.2.3.a	Outsourcing	the approval from SAMA prior to material outsourcing;	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
3.4.2.3.b	Outsourcing	the involvement of the cyber security function;	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
3.4.2.3.c	Outsourcing	compliance with the SAMA circular on outsourcing.	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
3.4.3	Cloud Computing	The Member Organization should define, implement and monitor the required cyber security controls within the cloud computing policy and process for hybrid and public cloud services. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.1	Cloud Computing	The cyber security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and implemented and communicated within Member Organization.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.2	Cloud Computing	The compliance with the cloud computing policy should be monitored.	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	
3.4.3.3	Cloud Computing	The cyber security controls regarding the cloud computing policy and process for hybrid and public cloud services should be periodically measured and evaluated.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4	Cloud Computing	The cloud computing policy for hybrid and public cloud services should address requirements for:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.a	Cloud Computing	the process for adopting cloud services, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.a.1	Cloud Computing	a cyber security risk assessment and due diligence on the cloud service provider and its cloud services should be performed;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.a.2	Cloud Computing	the Member Organization should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.a.3	Cloud Computing	a contract should be in place, including the cyber security requirements, before using cloud services;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.b	Cloud Computing	data location, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.b.1	Cloud Computing	in principle only cloud services should be used that are located in Saudi Arabia, or when cloud services are to be used outside Saudi Arabia that the Member Organization should obtain explicit approval from SAMA;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.c	Cloud Computing	data use limitations, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.c.1	Cloud Computing	the cloud service provider should not use the Member Organization's data for secondary purposes;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.d	Cloud Computing	security, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.d.1	Cloud Computing	the cloud service provider should implement and monitor the cyber security controls as determined in the risk assessment for protecting the confidentiality, integrity and availability of the Member Organization's data;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.e	Cloud Computing	data segregation, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.e.1	Cloud Computing	the Member Organization's data is logically segregated from other data held by the cloud service provider, including that the cloud service provider should be able to identify the Member Organization's data and at all times should be able to distinguish it from other data.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.f	Cloud Computing	business continuity, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.f.1	Cloud Computing	business continuity requirements are met in accordance with the Member Organization's business continuity policy;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.g	Cloud Computing	audit, review and monitoring, including that:	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.g.1	Cloud Computing	the Member Organization has the right to perform a cyber security review at the cloud service provider;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.g.2	Cloud Computing	the Member Organization has the right to perform a cyber security audit at the cloud service provider;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.g.3	Cloud Computing	the Member Organization has the right to perform a cyber security examination at the cloud service provider;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
3.4.3.4.h	Cloud Computing	exit, including that:	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	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: Saudi Arabia - Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework Version 1.0 (2017)
Focal Document URL: https://rulebook.sama.gov.sa/en/cyber-security-framework-2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sama-csf-1-2017.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
3.4.3.4.h.1	Cloud Computing	the Member Organization has termination rights;	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
3.4.3.4.h.2	Cloud Computing	the cloud service provider has to return the Member Organization's data on termination;	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
3.4.3.4.h.3	Cloud Computing	the cloud service provider has to irreversibly delete the Member Organization's data on termination.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	