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 - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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	Cybersecurity Governance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
1-1	Cybersecurity Strategy	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control are: (1) Implemented correctly; and (2) Operating as intended.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	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.	8	
1-1-1	Cybersecurity Strategy	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	8	
1-2	Cybersecurity Risk Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-2-1	Cybersecurity Risk Management	In addition to the controls in ECC subdomain 1-5, cybersecurity risk management methodology must include at least the following:	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	
1-2-1	Cybersecurity Risk Management	In addition to the controls in ECC subdomain 1-5, cybersecurity risk management methodology must include at least the following:	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
1-2-1-1	Cybersecurity Risk Management	Conducting a cybersecurity risk assessment on critical systems at least once annually.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
1-2-1-2	Cybersecurity Risk Management	Creating a cybersecurity risk register for critical systems, and reviewing it at least once every month.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
1-3	Cybersecurity in Information Technology Project Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-3-1	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-2, cybersecurity requirements of project management and asset (information technology) change management of the organization's critical systems must include at least the following:	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
1-3-1	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-2, cybersecurity requirements of project management and asset (information technology) change management of the organization's critical systems must include at least the following:	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
1-3-1	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-2, cybersecurity requirements of project management and asset (information technology) change management of the organization's critical systems must include at least the following:	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
1-3-1	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-2, cybersecurity requirements of project management and asset (information technology) change management of the organization's critical systems must include at least the following:	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
1-3-1-1	Cybersecurity in Information Technology Project Management	Conducting a stress test to ensure the capacity of the various components.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	8	
1-3-1-1	Cybersecurity in Information Technology Project Management	Conducting a stress test to ensure the capacity of the various components.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3	
1-3-1-1	Cybersecurity in Information Technology Project Management	Conducting a stress test to ensure the capacity of the various components.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	8	
1-3-1-2	Cybersecurity in Information Technology Project Management	Ensuring the implementation of business continuity requirements.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
1-3-1-2	Cybersecurity in Information Technology Project Management	Ensuring the implementation of business continuity requirements.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	

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 - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
1-3-2	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-3, cybersecurity requirements related to software and application development projects of the organization's critical systems must include at least the following:	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
1-3-2	Cybersecurity in Information Technology Project Management	In addition to the subcontrols in ECC control 1-6-3, cybersecurity requirements related to software and application development projects of the organization's critical systems must include at least the following:	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
1-3-2-1	Cybersecurity in Information Technology Project Management	Conducting a security source code review before the critical system release.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	8	
1-3-2-1	Cybersecurity in Information Technology Project Management	Conducting a security source code review before the critical system release.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	8	
1-3-2-1	Cybersecurity in Information Technology Project Management	Conducting a security source code review before the critical system release.	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
1-3-2-1	Cybersecurity in Information Technology Project Management	Conducting a security source code review before the critical system release.	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
1-3-2-2	Cybersecurity in Information Technology Project Management	Securing the access, storage, documentation and releases of source code.	Functional	Intersects With	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	5	
1-3-2-2	Cybersecurity in Information Technology Project Management	Securing the access, storage, documentation and releases of source code.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	8	
1-3-2-2	Cybersecurity in Information Technology Project Management	Securing the access, storage, documentation and releases of source code.	Functional	Intersects With	Software Escrow	TDA-20.3	Mechanisms exist to escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support.	3	
1-3-2-3	Cybersecurity in Information Technology Project Management	Securing the authenticated Application Programming Interface (API).	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
1-3-2-3	Cybersecurity in Information Technology Project Management	Securing the authenticated Application Programming Interface (API).	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.	3	
1-3-2-3	Cybersecurity in Information Technology Project Management	Securing the authenticated Application Programming Interface (API).	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3	
1-3-2-4	Cybersecurity in Information Technology Project Management	Secure and trusted migration of applications from testing environments to production environments, along with deletion of any data, IDs or passwords related to the testing environment before the migration.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
1-3-2-4	Cybersecurity in Information Technology Project Management	Secure and trusted migration of applications from testing environments to production environments, along with deletion of any data, IDs or passwords related to the testing environment before the migration.	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	
1-3-2-4	Cybersecurity in Information Technology Project Management	Secure and trusted migration of applications from testing environments to production environments, along with deletion of any data, IDs or passwords related to the testing environment before the migration.	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	8	
1-4	Periodical Cybersecurity Review and Audit	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-4-1	Periodical Cybersecurity Review and Audit	With reference to ECC control 1-8-1, the organization's cybersecurity function must review the implementation of CSCC at least once annually.	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.	8	
1-4-2	Periodical Cybersecurity Review and Audit	With reference to ECC control 1-8-2, the implementation of CSCC must be reviewed by independent parties within the organization, outside the cybersecurity function at least once every three years.	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	
1-4-2	Periodical Cybersecurity Review and Audit	With reference to ECC control 1-8-2, the implementation of CSCC must be reviewed by independent parties within the organization, outside the cybersecurity function at least once every three years.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	8	
1-5	Cybersecurity in Human Resources	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-5-1	Cybersecurity in Human Resources	In addition to the subcontrols in ECC control 1-9-3, personnel cybersecurity requirements prior to employment must include at least the following:	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-5-1-1	Cybersecurity in Human Resources	Screening or vetting candidates for working on critical systems.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
1-5-1-2	Cybersecurity in Human Resources	The technical support and development positions for critical systems, must be filled with experienced Saudi professionals.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
1-5-1-2	Cybersecurity in Human Resources	The technical support and development positions for critical systems, must be filled with experienced Saudi professionals.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
2	Cybersecurity Defense	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2-1	Asset Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-1-1	Asset Management	In addition to the controls in ECC subdomain 2-1, cybersecurity requirements for managing information technology assets must include at least the following:	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
2-1-1-1	Asset Management	Maintaining an annually-updated inventory of critical systems' assets.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
2-1-1-1	Asset Management	Maintaining an annually-updated inventory of critical systems' assets.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
2-1-1-2	Asset Management	Identifying assets owners and involving them in the asset management lifecycle for critical systems.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
2-1-1-2	Asset Management	Identifying assets owners and involving them in the asset management lifecycle for critical systems.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	8	
2-2	Identity and Access Management	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 - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-2-1	Identity and Access Management	In addition to the subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management of critical systems must include at least the following:	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
2-2-1-1	Identity and Access Management	Prohibiting remote access from outside the Kingdom of Saudi Arabia.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8	
2-2-1-1	Identity and Access Management	Prohibiting remote access from outside the Kingdom of Saudi Arabia.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
2-2-1-2	Identity and Access Management	Restricting remote access from inside the Kingdom of Saudi Arabia and verifying each access attempt by the organization's security operations center, and continuously monitoring activities related to remote access.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8	
2-2-1-2	Identity and Access Management	Restricting remote access from inside the Kingdom of Saudi Arabia and verifying each access attempt by the organization's security operations center, and continuously monitoring activities related to remote access.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	8	
2-2-1-2	Identity and Access Management	Restricting remote access from inside the Kingdom of Saudi Arabia and verifying each access attempt by the organization's security operations center, and continuously monitoring activities related to remote access.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
2-2-1-3	Identity and Access Management	Using multi-factor authentication for all users.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8	
2-2-1-3	Identity and Access Management	Using multi-factor authentication for all users.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
2-2-1-4	Identity and Access Management	Using multi-factor authentication for privileged users, and on systems utilized for managing critical systems stated in control 2-3-1-4.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8	
2-2-1-4	Identity and Access Management	Using multi-factor authentication for privileged users, and on systems utilized for managing critical systems stated in control 2-3-1-4.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	8	
2-2-1-4	Identity and Access Management	Using multi-factor authentication for privileged users, and on systems utilized for managing critical systems stated in control 2-3-1-4.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	8	
2-2-1-5	Identity and Access Management	Developing and implementing a high-standard and secure password policy.	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	
2-2-1-5	Identity and Access Management	Developing and implementing a high-standard and secure password policy.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
2-2-1-6	Identity and Access Management	Utilizing secure methods and algorithms for storing and processing passwords, such as: Hashing functions.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2-2-1-6	Identity and Access Management	Utilizing secure methods and algorithms for storing and processing passwords, such as: Hashing functions.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
2-2-1-6	Identity and Access Management	Utilizing secure methods and algorithms for storing and processing passwords, such as: Hashing functions.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	8	
2-2-1-7	Identity and Access Management	Securely managing service accounts for applications and systems, and disabling interactive login from these accounts.	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	8	
2-2-1-7	Identity and Access Management	Securely managing service accounts for applications and systems, and disabling interactive login from these accounts.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and	8	
2-2-1-7	Identity and Access Management	Securely managing service accounts for applications and systems, and disabling interactive login from these accounts.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
2-2-1-8	Identity and Access Management	Prohibiting direct access and interaction with databases for all users except for database administrators. Users' access and interaction with databases must be through applications only, with consideration given to applying security solutions that limit or prohibit visibility of classified data to database administrators.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	8	
2-2-1-8	Identity and Access Management	Prohibiting direct access and interaction with databases for all users except for database administrators. Users' access and interaction with databases must be through applications only, with consideration given to applying security solutions that limit or prohibit visibility of classified data to database administrators.	Functional	Intersects With	Database Access	IAC-20.2	Mechanisms exist to restrict access to databases containing sensitive and/or regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires such access.	5	
2-2-1-8	Identity and Access Management	Prohibiting direct access and interaction with databases for all users except for database administrators. Users' access and interaction with databases must be through applications only, with consideration given to applying security solutions that limit or prohibit visibility of classified data to database administrators.	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
2-2-2	Identity and Access Management	With reference to ECC subcontrol 2-2-3-5, user identities and access rights to critical systems must be reviewed at least once every three months.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
2-3	Information System and Information Processing Facilities Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-3-1	Information System and Information Processing Facilities Protection	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for protecting critical systems and information processing facilities must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-3-1-1	Information System and Information Processing Facilities Protection	Whitelisting of application and software operation files that are allowed to execute on servers hosting critical systems.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	8	
2-3-1-2	Information System and Information Processing Facilities Protection	Protecting servers hosting critical systems using end-point protection solutions that are approved by the organization.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
2-3-1-2	Information System and Information Processing Facilities Protection	Protecting servers hosting critical systems using end-point protection solutions that are approved by the organization.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	8	
2-3-1-3	Information System and Information Processing Facilities Protection	Applying security patches and updates at least once every month for external and internet-connected critical systems and at least once every three months for internal critical systems, in line with the organization's approved change managmenet mechanisms.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
2-3-1-3	Information System and Information Processing Facilities Protection	Applying security patches and updates at least once every month for external and internet-connected critical systems and at least once every three months for internal critical systems, in line with the organization's approved change managmenet mechanisms.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
2-3-1-4	Information System and Information Processing Facilities Protection	Allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services (e.g., email service or internet), to be used by highly privileged accounts.	Functional	Intersects With	Jump Server	AST-27	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.	5	
2-3-1-4	Information System and Information Processing Facilities Protection	Allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services (e.g., email service or internet), to be used by highly privileged accounts.	Functional	Intersects With	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	8	
2-3-1-4	Information System and Information Processing Facilities Protection	Allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services (e.g., email service or internet), to be used by highly privileged accounts.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	8	
2-3-1-4	Information System and Information Processing Facilities Protection	Allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services (e.g., email service or internet), to be used by highly privileged accounts.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	8	

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

Focal Document: Saudi Arabia - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-3-1-5	Information System and Information Processing Facilities Protection	Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2-3-1-5	Information System and Information Processing Facilities Protection	Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	3	
2-3-1-5	Information System and Information Processing Facilities Protection	Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	
2-3-1-5	Information System and Information Processing Facilities Protection	Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
2-3-1-6	Information System and Information Processing Facilities Protection	Reviewing critical systems' configurations and hardening at least once every six months.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	
2-3-1-6	Information System and Information Processing Facilities Protection	Reviewing critical systems' configurations and hardening at least once every six months.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2-3-1-6	Information System and Information Processing Facilities Protection	Reviewing critical systems' configurations and hardening at least once every six months.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
2-3-1-6	Information System and Information Processing Facilities Protection	Reviewing critical systems' configurations and hardening at least once every six months.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
2-3-1-7	Information System and Information Processing Facilities Protection	Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords, where applicable.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2-3-1-7	Information System and Information Processing Facilities Protection	Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords, where applicable.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
2-3-1-8	Information System and Information Processing Facilities Protection	Protecting systems' logs and critical files from unauthorized access, tampering, illegitimate modification and/or deletion.	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	
2-4	Networks Security Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-4-1	Networks Security Management	In addition to the subcontrols in ECC control 2-5-3, cybersecurity requirements of critical systems' network security management must include at least the following:	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-4-1-1	Networks Security Management	Logically and/or physically segregating and isolating critical systems' networks.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	8	
2-4-1-2	Networks Security Management	Reviewing firewall rules and access lists, at least once every six months.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
2-4-1-2	Networks Security Management	Reviewing firewall rules and access lists, at least once every six months.	Functional	Intersects With	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.	3	
2-4-1-3	Networks Security Management	Prohibiting direct connection between local network devices and critical systems, unless those devices are scanned to ensure they have security controls that meet the acceptable security levels for critical systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
2-4-1-3	Networks Security Management	Prohibiting direct connection between local network devices and critical systems, unless those devices are scanned to ensure they have security controls that meet the acceptable security levels for critical systems.	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive and/or regulated data enclaves (secure zones).	8	
2-4-1-3	Networks Security Management	Prohibiting direct connection between local network devices and critical systems, unless those devices are scanned to ensure they have security controls that meet the acceptable security levels for critical systems.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
2-4-1-4	Networks Security Management	Prohibiting critical systems from connecting to a wireless network.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
2-4-1-4	Networks Security Management	Prohibiting critical systems from connecting to a wireless network.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	8	
2-4-1-4	Networks Security Management	Prohibiting critical systems from connecting to a wireless network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
2-4-1-4	Networks Security Management	Prohibiting critical systems from connecting to a wireless network.	Functional	Intersects With	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	5	
2-4-1-5	Networks Security Management	Protecting against Advanced Persistent Threats (APT) at the network layer.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	8	
2-4-1-5	Networks Security Management	Protecting against Advanced Persistent Threats (APT) at the network layer.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	8	
2-4-1-6	Networks Security Management	Prohibiting connection to the internet for critical systems that provide internal services to the organization and have no strong need to be accessed from outside the organization.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
2-4-1-6	Networks Security Management	Prohibiting connection to the internet for critical systems that provide internal services to the organization and have no strong need to be accessed from outside the organization.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	8	
2-4-1-6	Networks Security Management	Prohibiting connection to the internet for critical systems that provide internal services to the organization and have no strong need to be accessed from outside the organization.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	5	
2-4-1-6	Networks Security Management	Prohibiting connection to the internet for critical systems that provide internal services to the organization and have no strong need to be accessed from outside the organization.	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive and/or regulated data enclaves (secure zones).	8	
2-4-1-7	Networks Security Management	Critical systems that provide services to a limited number of organizations (not individuals), shall use networks isolated from the Internet.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
2-4-1-7	Networks Security Management	Critical systems that provide services to a limited number of organizations (not individuals), shall use networks isolated from the Internet.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
2-4-1-7	Networks Security Management	Critical systems that provide services to a limited number of organizations (not individuals), shall use networks isolated from the Internet.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	8	
2-4-1-8	Networks Security Management	Protecting against Distributed Denial of Service (DDoS) attacks to limit risks arising from these attacks.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	8	
2-4-1-9	Networks Security Management	Allowing only whitelisting for critical systems' firewall access lists.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
2-4-1-9	Networks Security Management	Allowing only whitelisting for critical systems' firewall access lists.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	8	
2-5	Mobile Devices Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-5-1	Mobile Devices Security	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices security and BYOD in the organization must include at least the following:	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
2-5-1-1	Mobile Devices Security	Prohibting access to critical systems from mobile devices except for a temporary period only, after assessing the risks and obtaining the necessary approvals from the cybersecurity function in the organization.	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	8	

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

Focal Document: Saudi Arabia - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-5-1-1	Mobile Devices Security	Prohibting access to critical systems from mobile devices except for a temporary period only, after assessing the risks and obtaining the necessary approvals from the cybersecurity function in the organization.	Functional	Intersects With	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).	8	
2-5-1-2	Mobile Devices Security	Implementing full disk encryption for mobile devices with access to critical systems.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
2-6	Data and Information Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-6-1	Data and Information Protection	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for protecting and handling data and information must include at least the following:	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
2-6-1-1	Data and Information Protection	Prohibting the use of critical systems' data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
2-6-1-1	Data and Information Protection	Prohibting the use of critical systems' data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	8	
2-6-1-1	Data and Information Protection	Prohibting the use of critical systems' data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.	8	
2-6-1-1	Data and Information Protection	Prohibting the use of critical systems' data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.	Functional	Intersects With	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that Technology Assets, Applications and/or Services (TAAS) are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	3	
2-6-1-1	Data and Information Protection	Prohibting the use of critical systems' data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.	Functional	Intersects With	Data Anonymization	PRI-05.3	Mechanisms exist to mask sensitive and/or regulated data through data anonymization, pseudonymization, redaction and/or de-identification.	8	
2-6-1-2	Data and Information Protection	Classifying all data within critical systems.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
2-6-1-3	Data and Information Protection	Protecting classified data of critical systems using data leakage prevention techniques.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
2-6-1-3	Data and Information Protection	Protecting classified data of critical systems using data leakage prevention techniques.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
2-6-1-3	Data and Information Protection	Protecting classified data of critical systems using data leakage prevention techniques.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
2-6-1-3	Data and Information Protection	Protecting classified data of critical systems using data leakage prevention techniques.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.	8	
2-6-1-3	Data and Information Protection	Protecting classified data of critical systems using data leakage prevention techniques.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.	5	
2-6-1-4	Data and Information Protection	Identifying retention period for critical systems-associated data, in accordance with relevant legislations. Only required data must be retained in critical systems' production environments.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
2-6-1-5	Data and Information Protection	Prohibting the transfer of any critical systems' data from production environment to any other environment.	Functional	Intersects With	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive and/or regulated media that is transferred outside of the organization's facilities.	5	
2-6-1-5	Data and Information Protection	Prohibting the transfer of any critical systems' data from production environment to any other environment.	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	5	
2-6-1-5	Data and Information Protection	Prohibting the transfer of any critical systems' data from production environment to any other environment.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
2-6-1-5	Data and Information Protection	Prohibting the transfer of any critical systems' data from production environment to any other environment.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	5	
2-6-1-5	Data and Information Protection	Prohibting the transfer of any critical systems' data from production environment to any other environment.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
2-7	Cryptography	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-7-1	Cryptography	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must include at least the following:	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	
2-7-1-1	Cryptography	Encrypting all critical systems' data-in-transit.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2-7-1-1	Cryptography	Encrypting all critical systems' data-in-transit.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	3	
2-7-1-2	Cryptography	Encrypting all critical systems' data-at-rest at the level of files, database or certain columns within database.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
2-7-1-3	Cryptography	Using secure and up-to-date methods, algorithms, keys and devices in accordance with what NCA issues in this regard.	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.	8	
2-7-1-3	Cryptography	Using secure and up-to-date methods, algorithms, keys and devices in accordance with what NCA issues in this regard.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5	
2-8	Backup and Recovery Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-8-1	Backup and Recovery Management	In addition to the subcontrols in ECC control 2-9-3, cybersecurity requirements for backup and recovery management must include at least the following:	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
2-8-1-1	Backup and Recovery Management	Scope and coverage of online and offline backups shall cover all critical systems.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
2-8-1-1	Backup and Recovery Management	Scope and coverage of online and offline backups shall cover all critical systems.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
2-8-1-2	Backup and Recovery Management	Performing backup within planned intervals, according to the organization's risk assessment. NCA recommends performing backup for critical systems on a daily basis.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
2-8-1-3	Backup and Recovery Management	Securing access, storage and transfer of critical systems' backups and storage media, and protecting it from destruction, unauthorized access or modification.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
2-8-1-3	Backup and Recovery Management	Securing access, storage and transfer of critical systems' backups and storage media, and protecting it from destruction, unauthorized access or modification.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
2-8-1-3	Backup and Recovery Management	Securing access, storage and transfer of critical systems' backups and storage media, and protecting it from destruction, unauthorized access or modification.	Functional	Intersects With	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	8	
2-8-1-3	Backup and Recovery Management	Securing access, storage and transfer of critical systems' backups and storage media, and protecting it from destruction, unauthorized access or modification.	Functional	Intersects With	Backup Modification and/or Destruction	BCD-11.10	Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles.	8	
2-8-2	Backup and Recovery Management	With reference to ECC subcontrol 2-9-3-3, a periodical test must be conducted at least once every three months in order to determine the efficiency of recovering critical systems backups.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	

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

Focal Document: Saudi Arabia - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-8-2	Backup and Recovery Management	With reference to ECC subcontrol 2-9-3-3, a periodical test must be conducted at least once every three months in order to determine the efficiency of recovering critical systems backups.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
2-9	Vulnerabilities Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-9-1	Vulnerabilities Management	In addition to the subcontrols in ECC control 2-10-3, cybersecurity requirements for technical vulnerabilities management of critical systems must include at least the following:	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-9-1-1	Vulnerabilities Management	Utilizing trusted methods and tools for vulnerabilities assessments.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
2-9-1-1	Vulnerabilities Management	Utilizing trusted methods and tools for vulnerabilities assessments.	Functional	Intersects With	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	3	
2-9-1-1	Vulnerabilities Management	Utilizing trusted methods and tools for vulnerabilities assessments.	Functional	Intersects With	Internal Vulnerability Assessment Scans	VPM-06.7	Mechanisms exist to perform quarterly internal vulnerability scans, which includes all segments of the organization's internal network, as well as rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	3	
2-9-1-2	Vulnerabilities Management	Assessing and remediating vulnerabilities (by installing security updates and patches) on technical components of critical systems at least once every month for external and internet-connected critical systems, and at least once every three months for internal critical systems.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
2-9-1-2	Vulnerabilities Management	Assessing and remediating vulnerabilities (by installing security updates and patches) on technical components of critical systems at least once every month for external and internet-connected critical systems, and at least once every three months for internal critical systems.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
2-9-1-3	Vulnerabilities Management	Immediately remediating for critical vulnerabilities, in line with change management processes approved by the organization.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	
2-9-2	Vulnerabilities Management	With reference to ECC subcontrol 2-10-3-1, vulnerabilities assessments must be conducted on critical systems' technical components at least once every month.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
2-9-2	Vulnerabilities Management	With reference to ECC subcontrol 2-10-3-1, vulnerabilities assessments must be conducted on critical systems' technical components at least once every month.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
2-9-2	Vulnerabilities Management	With reference to ECC subcontrol 2-10-3-1, vulnerabilities assessments must be conducted on critical systems' technical components at least once every month.	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	5	
2-10	Penetration Testing	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-10-1	Penetration Testing	In addition to the subcontrols in ECC control 2-11-3, cybersecurity requirements for penetration testing on critical systems must include at least the following:	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-10-1-1	Penetration Testing	Scope of penetration tests must cover all of the critical systems' technical components and all its internal and external services.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
2-10-1-1	Penetration Testing	Scope of penetration tests must cover all of the critical systems' technical components and all its internal and external services.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
2-10-1-2	Penetration Testing	Conducting penetration tests by a qualified team.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
2-10-1-2	Penetration Testing	Conducting penetration tests by a qualified team.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	8	
2-10-2	Penetration Testing	With reference to ECC subcontrol 2-11-3-2, penetration tests must be conducted on critical systems at least once every six months.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
2-11	Cybersecurity Event Logs and Monitoring Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-11-1	Cybersecurity Event Logs and Monitoring Management	In addition to the subcontrols in ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for critical systems must include at least the following:	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2-11-1-1	Cybersecurity Event Logs and Monitoring Management	Activating cybersecurity event logs on all technical components of critical systems.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	8	
2-11-1-2	Cybersecurity Event Logs and Monitoring Management	Activating and monitoring of alerts and event logs related to file integrity management.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Monitoring and analyzing user behavior.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	8	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Monitoring and analyzing user behavior.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Monitoring and analyzing user behavior.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Monitoring and analyzing user behavior.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Monitoring and analyzing user behavior.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	8	
2-11-1-4	Cybersecurity Event Logs and Monitoring Management	Monitoring critical systems security events around the clock.	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	
2-11-1-4	Cybersecurity Event Logs and Monitoring Management	Monitoring critical systems security events around the clock.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	8	
2-11-1-4	Cybersecurity Event Logs and Monitoring Management	Monitoring critical systems security events around the clock.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
2-11-1-5	Cybersecurity Event Logs and Monitoring Management	Maintaining and protecting critical systems security events logs. The log shall include all details (e.g., time, date, ID and affected system).	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.	8	
2-11-1-5	Cybersecurity Event Logs and Monitoring Management	Maintaining and protecting critical systems security events logs. The log shall include all details (e.g., time, date, ID and affected system).	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	8	
2-11-1-5	Cybersecurity Event Logs and Monitoring Management	Maintaining and protecting critical systems security events logs. The log shall include all details (e.g., time, date, ID and affected system).	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	8	
2-11-2	Cybersecurity Event Logs and Monitoring Management	With reference to ECC subcontrol 2-12-3-5, retention period of cybersecurity's critical systems event logs must be 18 months minimum, in accordance with relevant legislative and regulatory requirements.	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	
2-11-2	Cybersecurity Event Logs and Monitoring Management	With reference to ECC subcontrol 2-12-3-5, retention period of cybersecurity's critical systems event logs must be 18 months minimum, in accordance with relevant legislative and regulatory requirements.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	3	

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

Focal Document: Saudi Arabia - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-11-2	Cybersecurity Event Logs and Monitoring Management	With reference to ECC subcontrol 2-12-3-5, retention period of cybersecurity's critical systems event logs must be 18 months minimum, in accordance with relevant legislative and regulatory requirements.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	
2-11-2	Cybersecurity Event Logs and Monitoring Management	With reference to ECC subcontrol 2-12-3-5, retention period of cybersecurity's critical systems event logs must be 18 months minimum, in accordance with relevant legislative and regulatory requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
2-12	Web Application Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-12-1	Web Application Security	In addition to the subcontrols in ECC control 2-15-3, cybersecurity requirements for external web applications for the organization's critical systems must include at least the following:	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	
2-12-1	Web Application Security	In addition to the subcontrols in ECC control 2-15-3, cybersecurity requirements for external web applications for the organization's critical systems must include at least the following:	Functional	Subset Of	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.	10	
2-12-1-1	Web Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	5	
2-12-1-1	Web Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-	5	
2-12-1-1	Web Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	8	
2-12-1-1	Web Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Intersects With	Web Application Framework	WEB-08	Mechanisms exist to use a robust Web Application Framework to support the development of secure web applications, including web services, web resources and web Application Programming Interfaces	5	
2-12-1-1	Web Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Intersects With	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5	
2-12-1-2	Web Application Security	Applying the minimum standards of Open Web Application Security Project (OWASP) Top Ten.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	5	
2-12-1-2	Web Application Security	Applying the minimum standards of Open Web Application Security Project (OWASP) Top Ten.	Functional	Intersects With	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	8	
2-12-2	Web Application Security	With reference to ECC subcontrol 2-15-3-2, multi-tier architecture principle, with minimum 3 tiers, must be used.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
2-12-2	Web Application Security	With reference to ECC subcontrol 2-15-3-2, multi-tier architecture principle, with minimum 3 tiers, must be used.	Functional	Intersects With	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	8	
2-13	Application Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Security, Compliance & Resilience Protection	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve	8	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience	8	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	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.	8	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:	5	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
2-13-1	Application Security	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
2-13-2	Application Security	The cybersecurity requirements for critical systems' internal applications must be implemented.	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	8	
2-13-2	Application Security	The cybersecurity requirements for critical systems' internal applications must be implemented.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the	5	
2-13-2	Application Security	The cybersecurity requirements for critical systems' internal applications must be implemented.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:	5	
2-13-2	Application Security	The cybersecurity requirements for critical systems' internal applications must be implemented.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
2-13-2	Application Security	The cybersecurity requirements for critical systems' internal applications must be implemented.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
2-13-3	Application Security	The cybersecurity requirements for critical systems' internal applications must include at least the following:	Functional	Subset Of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable	10	
2-13-3-1	Application Security	Adopting multi-tier architecture principle, provided that number of tiers is not less than three.	Functional	Subset Of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	10	
2-13-3-2	Application Security	Using secure protocols (e.g., HTTPS).	Functional	Subset Of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	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 - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.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
2-13-3-3	Application Security	Outlining the acceptable use policy for users.	Functional	Subset Of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	10	
2-13-3-4	Application Security	Secure session management, including session authenticity, session lockout and session timeout.	Functional	Subset Of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	10	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	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;	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	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	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	8	
2-13-4	Application Security	The cybersecurity requirements for critical systems' internal applications must be reviewed periodically.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
3	Cybersecurity Resilience	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3-1	Cybersecurity Resilience Aspects of Business	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	In addition to the subcontrols in ECC control 3-1-3, cybersecurity requirements for business continuity management must include at least the following:	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	10	
3-1-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Establishing a disaster recovery center for critical systems.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3-1-1-2	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Incorporating critical systems within disaster recovery plans.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8	
3-1-1-2	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Incorporating critical systems within disaster recovery plans.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
3-1-1-3	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Conducting periodical tests to ensure the efficiency of disaster recovery plans for critical systems, at least once annually.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
3-1-1-4	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	NCA recommends conducting periodical live Disaster Recovery (DR) test for critical systems.	Functional	Intersects With	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	5	
3-1-1-4	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	NCA recommends conducting periodical live Disaster Recovery (DR) test for critical systems.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
4	Third-Party and Cloud Computing Cybersecurity	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4-1	Third-Party Cybersecurity	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
4-1-1	Third-Party Cybersecurity	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for contracts and agreements with third-parties must include	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their	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 - Critical Systems Cybersecurity Controls (CSCC – 1: 2019)
Focal Document URL: https://www.nca.gov.sa/en/legislation?item=194&slug=controls-list
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-cscc-1-2019.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's	5	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
4-1-1-1	Third-Party Cybersecurity	Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems.	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,	5	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's	8	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
4-1-1-2	Third-Party Cybersecurity	Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory 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,	5	
4-2	Cloud Computing and Hosting Cybersecurity	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
4-2-1	Cloud Computing and Hosting Cybersecurity	In addition to the subcontrols in ECC control 4-2-3, cybersecurity requirements related to the use of hosting and cloud computing services	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line	10	
4-2-1-1	Cloud Computing and Hosting Cybersecurity	Hosting of critical systems and any part of their technical components must be inside the organization or within cloud computing services provided by government organizations or Saudi companies that are in	Functional	Intersects With	Geolocation Requirements for Processing, Storage and	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	8	
4-2-1-1	Cloud Computing and Hosting Cybersecurity	Hosting of critical systems and any part of their technical components must be inside the organization or within cloud computing services provided by government organizations or Saudi companies that are in compliance with NCA's Cloud Cybersecurity Controls (CCC), taking into account the classification of the hosted data.	Functional	Intersects With	Data Localization	DCH-26	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	8	