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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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	A cybersecurity strategy must be defined, documented and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as Authorizing Official). The strategy goals must be in-line with related laws and regulations.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
1-1-1	Cybersecurity Strategy	A cybersecurity strategy must be defined, documented and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as Authorizing Official). The strategy goals must be in-line with related laws and regulations.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
1-1-1	Cybersecurity Strategy	A cybersecurity strategy must be defined, documented and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as Authorizing Official). The strategy goals must be in-line with related laws and regulations.	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	
1-1-2	Cybersecurity Strategy	A roadmap must be executed to implement the cybersecurity strategy.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and	5	
1-1-3	Cybersecurity Strategy	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
1-1-3	Cybersecurity Strategy	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
1-1-3	Cybersecurity Strategy	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	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	
1-1-3	Cybersecurity Strategy	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and	8	
1-1-3	Cybersecurity Strategy	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
1-2	Cybersecurity Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-2-1	Cybersecurity Management	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent from the Information Technology/Information Communication and Technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
1-2-2	Cybersecurity Management	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
1-2-3	Cybersecurity Management	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
1-2-3	Cybersecurity Management	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.	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	Cybersecurity Policies and Procedures	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-3-1	Cybersecurity Policies and Procedures	Cybersecurity policies and procedures must be defined and documented by the cybersecurity function, approved by the Authorizing Official, and disseminated to relevant parties inside and outside the organization.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
1-3-2	Cybersecurity Policies and Procedures	The cybersecurity function must ensure that the cybersecurity policies and procedures are implemented.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
1-3-2	Cybersecurity Policies and Procedures	The cybersecurity function must ensure that the cybersecurity policies and procedures are implemented.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
1-3-3	Cybersecurity Policies and Procedures	The cybersecurity policies and procedures must be supported by technical security standards (e.g., operating systems, databases and firewall technical security standards).	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	
1-3-3	Cybersecurity Policies and Procedures	The cybersecurity policies and procedures must be supported by technical security standards (e.g., operating systems, databases and firewall technical security standards).	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
1-3-4	Cybersecurity Policies and Procedures	The cybersecurity policies and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
1-3-4	Cybersecurity Policies and Procedures	The cybersecurity policies and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
1-3-4	Cybersecurity Policies and Procedures	The cybersecurity policies and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	
1-4	Cybersecurity Roles and Responsibilities	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-4-1	Cybersecurity Roles and Responsibilities	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
1-4-1	Cybersecurity Roles and Responsibilities	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	

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

Focal Document: Saudi Arabia - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
1-4-1	Cybersecurity Roles and Responsibilities	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1-4-1	Cybersecurity Roles and Responsibilities	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1-4-1	Cybersecurity Roles and Responsibilities	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1-4-2	Cybersecurity Roles and Responsibilities	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	8	
1-4-2	Cybersecurity Roles and Responsibilities	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1-4-2	Cybersecurity Roles and Responsibilities	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	3	
1-5	Cybersecurity Risk Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-5-1	Cybersecurity Risk Management	Cybersecurity risk management methodology and procedures must be defined, documented and approved as per confidentiality, integrity and availability considerations of information and technology assets.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with:	10	
1-5-1	Cybersecurity Risk Management	Cybersecurity risk management methodology and procedures must be defined, documented and approved as per confidentiality, integrity and availability considerations of information and technology assets.	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	
1-5-2	Cybersecurity Risk Management	The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	8	
1-5-2	Cybersecurity Risk Management	The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.	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	10	
1-5-2	Cybersecurity Risk Management	The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.	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	
1-5-3	Cybersecurity Risk Management	The cybersecurity risk assessment procedures must be implemented at least in the following cases:	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	
1-5-3	Cybersecurity Risk Management	The cybersecurity risk assessment procedures must be implemented at least in the following cases:	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	
1-5-3-1	Cybersecurity Risk Management	Early stages of technology projects.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
1-5-3-2	Cybersecurity Risk Management	Before making major changes to technology infrastructure.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
1-5-3-3	Cybersecurity Risk Management	During the planning phase of obtaining third party services.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
1-5-3-4	Cybersecurity Risk Management	During the planning phase and before going live for new technology services and products.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
1-5-4	Cybersecurity Risk Management	The cybersecurity risk management methodology and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.	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	10	
1-6	Cybersecurity in Information and Technology Project Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-6-1	Cybersecurity in Information and Technology Project Management	Cybersecurity requirements must be included in project and asset (information/ technology) change management methodology and procedures to identify and manage cybersecurity risks as part of project management lifecycle. The cybersecurity requirements must be a key part of the overall requirements of technology projects.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	8	
1-6-1	Cybersecurity in Information and Technology Project Management	Cybersecurity requirements must be included in project and asset (information/ technology) change management methodology and procedures to identify and manage cybersecurity risks as part of project management lifecycle. The cybersecurity requirements must be a key part of the overall requirements of technology projects.	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	
1-6-2	Cybersecurity in Information and Technology Project Management	The cybersecurity requirements in project and assets (information/technology) change management must include at least the following:	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
1-6-2-1	Cybersecurity in Information and Technology Project Management	Vulnerability assessment and remediation.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
1-6-2-1	Cybersecurity in Information and Technology Project Management	Vulnerability assessment and remediation.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
1-6-2-2	Cybersecurity in Information and Technology Project Management	Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	

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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
1-6-2-2	Cybersecurity in Information and Technology Project Management	Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
1-6-3	Cybersecurity in Information and Technology Project Management	The cybersecurity requirements related to software and application development projects must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
1-6-3-1	Cybersecurity in Information and Technology Project Management	Using secure coding standards.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
1-6-3-1	Cybersecurity in Information and Technology Project Management	Using secure coding standards.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
1-6-3-2	Cybersecurity in Information and Technology Project Management	Using trusted and licensed sources for software development tools and libraries.	Functional	Intersects With	Software Development Repository	CFG-09.3	Mechanisms exist to maintain an authoritative repository for software development activities that is separate from production software.	5	
1-6-3-2	Cybersecurity in Information and Technology Project Management	Using trusted and licensed sources for software development tools and libraries.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
1-6-3-3	Cybersecurity in Information and Technology Project Management	Conducting compliance test for software against the defined organizational cybersecurity requirements.	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	
1-6-3-3	Cybersecurity in Information and Technology Project Management	Conducting compliance test for software against the defined organizational cybersecurity requirements.	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
1-6-3-3	Cybersecurity in Information and Technology Project Management	Conducting compliance test for software against the defined organizational cybersecurity requirements.	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
1-6-3-3	Cybersecurity in Information and Technology Project Management	Conducting compliance test for software against the defined organizational cybersecurity requirements.	Functional	Intersects With	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	3	
1-6-3-3	Cybersecurity in Information and Technology Project Management	Conducting compliance test for software against the defined organizational cybersecurity requirements.	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	3	
1-6-3-4	Cybersecurity in Information and Technology Project Management	Secure integration between software components.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	3	
1-6-3-4	Cybersecurity in Information and Technology Project Management	Secure integration between software components.	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.	3	
1-6-3-4	Cybersecurity in Information and Technology Project Management	Secure integration between software components.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1-6-3-5	Cybersecurity in Information and Technology Project Management	Conducting a configurations' review, secure configuration and hardening and patching before going live for software products.	Functional	Subset Of	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.	10	
1-6-4	Cybersecurity in Information and Technology Project Management	The cybersecurity requirements in project management must be reviewed periodically.	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	8	
1-7	Compliance with Cybersecurity Standards, Laws and Regulations	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-7-1	Compliance with Cybersecurity Standards, Laws and Regulations	The organization must comply with related national cybersecurity laws and regulations.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1-7-2	Compliance with Cybersecurity Standards, Laws and Regulations	The organization must comply with any nationally-approved international agreements and commiments related to cybersecurity.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1-8	Periodical Cybersecurity Review and Audit	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-8-1	Periodical Cybersecurity Review and Audit	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.	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	
1-8-1	Periodical Cybersecurity Review and Audit	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
1-8-2	Periodical Cybersecurity Review and Audit	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	

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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
1-8-2	Periodical Cybersecurity Review and Audit	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.	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	
1-8-3	Periodical Cybersecurity Review and Audit	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official. Results must include the audit/review scope, observations, recommendations and remediation plans.	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	
1-8-3	Periodical Cybersecurity Review and Audit	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official. Results must include the audit/review scope, observations, recommendations and remediation plans.	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.	8	
1-8-3	Periodical Cybersecurity Review and Audit	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official. Results must include the audit/review scope, observations, recommendations and remediation plans.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8	
1-9	Cybersecurity in Human Resources	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-9-1	Cybersecurity in Human Resources	Personnel cybersecurity requirements (prior to employment, during employment and after termination/separation) must be defined, documented and approved.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-9-1	Cybersecurity in Human Resources	Personnel cybersecurity requirements (prior to employment, during employment and after termination/separation) must be defined, documented and approved.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1-9-1	Cybersecurity in Human Resources	Personnel cybersecurity requirements (prior to employment, during employment and after termination/separation) must be defined, documented and approved.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	8	
1-9-2	Cybersecurity in Human Resources	The personnel cybersecurity requirements must be implemented.	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	
1-9-2	Cybersecurity in Human Resources	The personnel cybersecurity requirements must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
1-9-2	Cybersecurity in Human Resources	The personnel cybersecurity requirements must be implemented.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-9-3	Cybersecurity in Human Resources	The 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	
1-9-3-1	Cybersecurity in Human Resources	Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	8	
1-9-3-1	Cybersecurity in Human Resources	Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
1-9-3-1	Cybersecurity in Human Resources	Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	8	
1-9-3-1	Cybersecurity in Human Resources	Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	8	
1-9-3-2	Cybersecurity in Human Resources	Screening or vetting candidates of cybersecurity and critical/privileged positions.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	
1-9-3-2	Cybersecurity in Human Resources	Screening or vetting candidates of cybersecurity and critical/privileged positions.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
1-9-4	Cybersecurity in Human Resources	The personnel cybersecurity requirements during 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	
1-9-4-1	Cybersecurity in Human Resources	Cybersecurity awareness (during on-boarding and during employment).	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	
1-9-4-1	Cybersecurity in Human Resources	Cybersecurity awareness (during on-boarding and during employment).	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
1-9-4-1	Cybersecurity in Human Resources	Cybersecurity awareness (during on-boarding and during employment).	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	8	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
1-9-4-2	Cybersecurity in Human Resources	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	8	
1-9-5	Cybersecurity in Human Resources	Personnel access to information and technology assets must be reviewed and removed immediately upon termination/separation.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
1-9-6	Cybersecurity in Human Resources	Personnel cybersecurity requirements must be reviewed periodically.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-10	Cybersecurity Awareness and Training Program	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-10-1	Cybersecurity Awareness and Training Program	A cybersecurity awareness program must be developed and approved. The program must be conducted periodically through multiple channels to strengthen the awareness about cybersecurity, cyber threats and risks, and to build a positive cybersecurity awareness culture.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
1-10-1	Cybersecurity Awareness and Training Program	A cybersecurity awareness program must be developed and approved. The program must be conducted periodically through multiple channels to strengthen the awareness about cybersecurity, cyber threats and risks, and to build a positive cybersecurity awareness culture.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
1-10-2	Cybersecurity Awareness and Training Program	The cybersecurity awareness program must be implemented.	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	
1-10-2	Cybersecurity Awareness and Training Program	The cybersecurity awareness program must be implemented.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
1-10-3	Cybersecurity Awareness and Training Program	The cybersecurity awareness program must cover the latest cyber threats and how to protect against them, and must include at least the following subjects:	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
1-10-3-1	Cybersecurity Awareness and Training Program	Secure handling of email services, especially phishing emails.	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	
1-10-3-1	Cybersecurity Awareness and Training Program	Secure handling of email services, especially phishing emails.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
1-10-3-2	Cybersecurity Awareness and Training Program	Secure handling of mobile devices and storage media.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5	
1-10-3-3	Cybersecurity Awareness and Training Program	Secure Internet browsing.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
1-10-3-4	Cybersecurity Awareness and Training Program	Secure use of social media.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
1-10-4	Cybersecurity Awareness and Training Program	Essential and customized (i.e., tailored to job functions as it relates to cybersecurity) training and access to professional skillsets must be made available to personnel working directly on tasks related to cybersecurity including:	Functional	No Relationship	N/A	N/A	N/A	0	
1-10-4-1	Cybersecurity Awareness and Training Program	Cybersecurity function's personnel.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1-10-4-2	Cybersecurity Awareness and Training Program	Personnel working on software/application development. and information and technology assets operations.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1-10-4-3	Cybersecurity Awareness and Training Program	Executive and supervisory positions.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1-10-5	Cybersecurity Awareness and Training Program	The implementation of the cybersecurity awareness program must be reviewed periodically.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
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	Cybersecurity requirements for managing information and technology assets must be defined, documented and approved.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
2-1-1	Asset Management	Cybersecurity requirements for managing information and technology assets must be defined, documented and approved.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
2-1-2	Asset Management	The cybersecurity requirements for managing information and technology assets must be implemented.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
2-1-2	Asset Management	The cybersecurity requirements for managing information and technology assets must be implemented.	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	
2-1-3	Asset Management	Acceptable use policy of information and technology assets must be defined, documented and approved.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
2-1-3	Asset Management	Acceptable use policy of information and technology assets must be defined, documented and approved.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
2-1-4	Asset Management	Acceptable use policy of information and technology assets must be implemented.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
2-1-4	Asset Management	Acceptable use policy of information and technology assets must be implemented.	Functional	Subset Of	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.	10	
2-1-4	Asset Management	Acceptable use policy of information and technology assets must be implemented.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
2-1-5	Asset Management	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
2-1-5	Asset Management	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.	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	
2-1-5	Asset Management	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-1-6	Asset Management	The cybersecurity requirements for managing information and technology assets must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-2	Identity and Access Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-2-1	Identity and Access Management	Cybersecurity requirements for identity and access management must be defined, documented and approved.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
2-2-1	Identity and Access Management	Cybersecurity requirements for identity and access management must be defined, documented and approved.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
2-2-2	Identity and Access Management	The cybersecurity requirements for identity and access management must be implemented.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
2-2-2	Identity and Access Management	The cybersecurity requirements for identity and access management must be implemented.	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	
2-2-3	Identity and Access Management	The cybersecurity requirements for identity and access management must include at least the following	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
2-2-3-1	Identity and Access Management	User authentication based on username and password.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
2-2-3-2	Identity and Access Management	Multi-factor authentication for remote access.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
2-2-3-3	Identity and Access Management	User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
2-2-3-4	Identity and Access Management	Privileged access management.	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).	5	
2-2-3-5	Identity and Access Management	Periodic review of users' identities and access rights.	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	
2-2-4	Identity and Access Management	The Implementation of the cybersecurity requirements for identity and access management must be reviewed periodically.	Functional	Subset Of	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	10	
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	Cybersecurity requirements for protecting information systems and information processing facilities must be defined, documented and approved.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-3-2	Information System and Information Processing Facilities Protection	The cybersecurity requirements for protecting information systems and information processing facilities must be implemented.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2-3-2	Information System and Information Processing Facilities Protection	The cybersecurity requirements for protecting information systems and information processing facilities must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
2-3-3	Information System and Information Processing Facilities Protection	The cybersecurity requirements for protecting information systems and information processing facilities must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-3-3-1	Information System and Information Processing Facilities Protection	Advanced, up-to-date and secure management of malware and virus protection on servers and workstations.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
2-3-3-2	Information System and Information Processing Facilities Protection	Restricted use and secure handling of external storage media.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
2-3-3-3	Information System and Information Processing Facilities Protection	Patch management for information systems, software and devices.	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.	5	
2-3-3-4	Information System and Information Processing Facilities Protection	Centralized clock synchronization with an accurate and trusted source (e.g., Saudi Standards, Metrology and Quality Organization (SASO)).	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
2-3-4	Information System and Information Processing Facilities Protection	The cybersecurity requirements for protecting information systems and information processing facilities must be reviewed periodically.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
2-4	Email Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-4-1	Email Protection	Cybersecurity requirements for protecting email service must be defined, documented and approved.	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	
2-4-2	Email Protection	The cybersecurity requirements for email service must be implemented.	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	
2-4-3	Email Protection	The cybersecurity requirements for protecting the email service must include at the least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-4-3-1	Email Protection	Analyzing and filtering email messages (specifically phishing emails and spam) using advanced and up-to-date email protection techniques.	Functional	Intersects With	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
2-4-3-2	Email Protection	Multi-factor authentication for remote and webmail access to email service.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
2-4-3-3	Email Protection	Email archiving and backup.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-4-3-4	Email Protection	Secure management and protection against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	Functional	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including: (1) Endpoints; (2) On-premises networks; (3) Cloud-based networks; (4) Electronic communications; (5) Applications; and (6) Services.	5	
2-4-3-5	Email Protection	Validation of the organization's email service domains (e.g., using Sender Policy Framework (SPF)).	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
2-4-4	Email Protection	The cybersecurity requirements for email service must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-5	Networks Security Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-5-1	Networks Security Management	Cybersecurity requirements for network security management must be defined, documented and approved.	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	
2-5-2	Networks Security Management	The cybersecurity requirements for network security management must be implemented.	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).	5	
2-5-2	Networks Security Management	The cybersecurity requirements for network security management must be implemented.	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	
2-5-3	Networks Security Management	The cybersecurity requirements for network security management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-5-3-1	Networks Security Management	Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles.	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.	5	
2-5-3-2	Networks Security Management	Network segregation between production, test and development environments.	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.	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
2-5-3-2	Networks Security Management	Network segregation between production, test and development environments.	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	
2-5-3-3	Networks Security Management	Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
2-5-3-4	Networks Security Management	Wireless network protection using strong authentication and encryption techniques. A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization's internal network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
2-5-3-4	Networks Security Management	Wireless network protection using strong authentication and encryption techniques. A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization's internal network.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
2-5-3-5	Networks Security Management	Management and restrictions on network services, protocols and ports.	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.	5	
2-5-3-6	Networks Security Management	Intrusion Prevention Systems (IPS).	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
2-5-3-7	Networks Security Management	Security of Domain Name Service (DNS).	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
2-5-3-8	Networks Security Management	Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
2-5-4	Networks Security Management	The cybersecurity requirements for network security management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-6	Mobile Devices Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-6-1	Mobile Devices Security	Cybersecurity requirements for mobile devices security and BYOD must be defined, documented and approved.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
2-6-1	Mobile Devices Security	Cybersecurity requirements for mobile devices security and BYOD must be defined, documented and approved.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
2-6-2	Mobile Devices Security	The cybersecurity requirements for mobile devices security and BYOD must be implemented.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
2-6-2	Mobile Devices Security	The cybersecurity requirements for mobile devices security and BYOD must be implemented.	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	
2-6-3	Mobile Devices Security	The cybersecurity requirements for mobile devices security and BYOD must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-6-3-1	Mobile Devices Security	Separation and encryption of organization's data and information stored on mobile devices and BYODs.	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	
2-6-3-2	Mobile Devices Security	Controlled and restricted use based on job requirements.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
2-6-3-3	Mobile Devices Security	Secure wiping of organization's data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization.	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
2-6-3-4	Mobile Devices Security	Security awareness for mobile devices users.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
2-6-4	Mobile Devices Security	The cybersecurity requirements for mobile devices security and BYOD must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-7	Data and Information Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-7-1	Data and Information Protection	Cybersecurity requirements for protecting and handling data and information must be defined, documented and approved as per the related laws and regulations.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
2-7-1	Data and Information Protection	Cybersecurity requirements for protecting and handling data and information must be defined, documented and approved as per the related laws and regulations.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	8	
2-7-1	Data and Information Protection	Cybersecurity requirements for protecting and handling data and information must be defined, documented and approved as per the related laws and regulations.	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	
2-7-2	Data and Information Protection	The cybersecurity requirements for protecting and handling data and information must be implemented.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated	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	
2-7-3	Data and Information Protection	The cybersecurity requirements for protecting and handling data and information must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-7-3-1	Data and Information Protection	Data and information ownership.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
2-7-3-2	Data and Information Protection	Data and information classification and labeling mechanisms.	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	5	
2-7-3-3	Data and Information Protection	Data and information privacy	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	
2-7-4	Data and Information Protection	The cybersecurity requirements for protecting and handling data and information must be reviewed periodically	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	5	
2-8	Cryptography	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-8-1	Cryptography	Cybersecurity requirements for cryptography must be defined, documented and approved.	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	10	
2-8-2	Cryptography	The cybersecurity requirements for cryptography must be implemented.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
2-8-2	Cryptography	The cybersecurity requirements for cryptography must be implemented.	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	5	
2-8-3	Cryptography	The cybersecurity requirements for cryptography must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-8-3-1	Cryptography	Approved cryptographic solutions standards and its technical and regulatory limitations.	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	10	
2-8-3-2	Cryptography	Secure management of cryptographic keys during their lifecycles	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	

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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
2-8-3-3	Cryptography	Encryption of data in-transit and at-rest as per classification and related laws and regulations.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
2-8-3-3	Cryptography	Encryption of data in-transit and at-rest as per classification and related laws and regulations.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
2-8-4	Cryptography	The cybersecurity requirements for cryptography must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at	5	
2-9	Backup and Recovery Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-9-1	Backup and Recovery Management	Cybersecurity requirements for backup and recovery management must be defined, documented and approved.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives	5	
2-9-1	Backup and Recovery Management	Cybersecurity requirements for backup and recovery management 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	5	
2-9-1	Backup and Recovery Management	Cybersecurity requirements for backup and recovery management must be defined, documented and approved.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable	5	
2-9-2	Backup and Recovery Management	The cybersecurity requirements for backup and recovery management must be implemented.	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	
2-9-2	Backup and Recovery Management	The cybersecurity requirements for backup and recovery management must be implemented.	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	
2-9-3	Backup and Recovery Management	The cybersecurity requirements for backup and recovery management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-9-3-1	Backup and Recovery Management	Scope and coverage of backups to cover critical technology and information assets.	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	5	
2-9-3-2	Backup and Recovery Management	Ability to perform quick recovery of data and systems after cybersecurity incidents.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-9-3-3	Backup and Recovery Management	Periodic tests of backup's recovery effectiveness.	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.	5	
2-9-4	Backup and Recovery Management	The cybersecurity requirements for backup and recovery management must be reviewed periodically	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	5	
2-10	Vulnerabilities Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-10-1	Vulnerabilities Management	Cybersecurity requirements for technical vulnerabilities management must be defined, documented and approved.	Functional	Subset Of	Vulnerability & Patch Management Program	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-10-2	Vulnerabilities Management	The cybersecurity requirements for technical vulnerabilities management must be implemented.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-10-2	Vulnerabilities Management	The cybersecurity requirements for technical vulnerabilities management must be implemented.	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	5	
2-10-3	Vulnerabilities Management	The cybersecurity requirements for technical vulnerabilities management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-10-3-1	Vulnerabilities Management	Periodic 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.	5	
2-10-3-2	Vulnerabilities Management	Vulnerabilities classification based on criticality level.	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	5	
2-10-3-3	Vulnerabilities Management	Vulnerabilities remediation based on classification and associated risk levels.	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	
2-10-3-4	Vulnerabilities Management	Security patch management.	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.	5	
2-10-3-5	Vulnerabilities Management	Subscription with authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
2-10-4	Vulnerabilities Management	The cybersecurity requirements for technical vulnerabilities management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at	5	
2-11	Penetration Testing	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-11-1	Penetration Testing	Cybersecurity requirements for penetration testing exercises must be defined, documented and approved.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-11-2	Penetration Testing	The cybersecurity requirements for penetration testing processes must be implemented.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-11-2	Penetration Testing	The cybersecurity requirements for penetration testing processes must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance &	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for	5	
2-11-3	Penetration Testing	The cybersecurity requirements for penetration testing processes must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-11-3-1	Penetration Testing	Scope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web	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	5	
2-11-3-1	Penetration Testing	Scope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-11-3-2	Penetration Testing	Conducting penetration tests periodically.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-11-4	Penetration Testing	Cybersecurity requirements for penetration testing processes must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at	5	
2-12	Cybersecurity Event Logs and Monitoring Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-12-1	Cybersecurity Event Logs and Monitoring Management	Cybersecurity requirements for event logs and monitoring management must be defined, documented and approved.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2-12-2	Cybersecurity Event Logs and Monitoring Management	The cybersecurity requirements for event logs and monitoring management must be implemented.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
2-12-2	Cybersecurity Event Logs and Monitoring Management	The cybersecurity requirements for event logs and monitoring management must be implemented.	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	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
2-12-3	Cybersecurity Event Logs and Monitoring Management	The cybersecurity requirements for event logs and monitoring management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-12-3-1	Cybersecurity Event Logs and Monitoring Management	Activation of cybersecurity event logs on critical information assets.	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.	5	
2-12-3-2	Cybersecurity Event Logs and Monitoring Management	Activation of cybersecurity event logs on remote access and privileged user accounts.	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.	5	
2-12-3-3	Cybersecurity Event Logs and Monitoring Management	Identification of required technologies (e.g., SIEM) for cybersecurity event logs collection.	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	
2-12-3-4	Cybersecurity Event Logs and Monitoring Management	Continuous monitoring of cybersecurity events.	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	
2-12-3-5	Cybersecurity Event Logs and Monitoring Management	Retention period for cybersecurity event logs (must be 12 months minimum).	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	5	
2-12-4	Cybersecurity Event Logs and Monitoring Management	The cybersecurity requirements for event logs and monitoring management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-13	Cybersecurity Incident and Threat Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-13-1	Cybersecurity Incident and Threat Management	Requirements for cybersecurity incidents and threat management must be defined, documented and approved.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability	8	
2-13-1	Cybersecurity Incident and Threat Management	Requirements for cybersecurity incidents and threat management must be defined, documented and approved.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures,	8	
2-13-2	Cybersecurity Incident and Threat Management	The requirements for cybersecurity incidents and threat management must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
2-13-2	Cybersecurity Incident and Threat Management	The requirements for cybersecurity incidents and threat management must be implemented.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	8	
2-13-2	Cybersecurity Incident and Threat Management	The requirements for cybersecurity incidents and threat management must be implemented.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures,	8	
2-13-3	Cybersecurity Incident and Threat Management	The requirements for cybersecurity incidents and threat management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-13-3-1	Cybersecurity Incident and Threat Management	Cybersecurity incident response plans and escalation procedures.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability	5	
2-13-3-1	Cybersecurity Incident and Threat Management	Cybersecurity incident response plans and escalation procedures.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
2-13-3-2	Cybersecurity Incident and Threat Management	Cybersecurity incidents classification.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business	8	
2-13-3-3	Cybersecurity Incident and Threat Management	Cybersecurity incidents reporting to NCA.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
2-13-3-3	Cybersecurity Incident and Threat Management	Cybersecurity incidents reporting to NCA.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
2-13-3-4	Cybersecurity Incident and Threat Management	Sharing incidents notifications, threat intelligence, breach indicators and reports with NCA.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
2-13-3-4	Cybersecurity Incident and Threat Management	Sharing incidents notifications, threat intelligence, breach indicators and reports with NCA.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
2-13-3-5	Cybersecurity Incident and Threat Management	Collecting and handling threat intelligence feeds.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures,	5	
2-13-3-5	Cybersecurity Incident and Threat Management	Collecting and handling threat intelligence feeds.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
2-13-4	Cybersecurity Incident and Threat Management	The requirements for cybersecurity incidents and threat management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-14	Physical Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-14-1	Physical Security	Cybersecurity requirements for physical protection of information and technology assets must be defined, documented and approved.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2-14-2	Physical Security	The cybersecurity requirements for physical protection of information and technology assets must be implemented.	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	8	
2-14-2	Physical Security	The cybersecurity requirements for physical protection of information and technology assets must be implemented.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2-14-3	Physical Security	The cybersecurity requirements for physical protection of information and technology assets must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
2-14-3-1	Physical Security	Authorized access to sensitive areas within the organization (e.g., data center, disaster recovery center, sensitive information processing facilities, security surveillance center, network cabinets).	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-14-3-2	Physical Security	Facility entry/exit records and CCTV monitoring.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-14-3-2	Physical Security	Facility entry/exit records and CCTV monitoring.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
2-14-3-2	Physical Security	Facility entry/exit records and CCTV monitoring.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	8	
2-14-3-3	Physical Security	Protection of facility entry/exit and surveillance records.	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	
2-14-3-3	Physical Security	Protection of facility entry/exit and surveillance records.	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	5	
2-14-3-3	Physical Security	Protection of facility entry/exit and surveillance records.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2-14-3-3	Physical Security	Protection of facility entry/exit and surveillance records.	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
2-14-3-4	Physical Security	Secure destruction and re-use of physical assets that hold classified information (including documents and storage media).	Functional	Subset Of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
2-14-3-5	Physical Security	Security of devices and equipment inside and outside the organization's facilities.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-14-3-5	Physical Security	Security of devices and equipment inside and outside the organization's facilities.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	
2-14-3-5	Physical Security	Security of devices and equipment inside and outside the organization's facilities.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
2-14-4	Physical Security	The cybersecurity requirements for physical protection of information and technology assets must be reviewed periodically.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
2-14-4	Physical Security	The cybersecurity requirements for physical protection of information and technology assets must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at	8	
2-15	Web Application Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-15-1	Web Application Security	Cybersecurity requirements for external web applications must be defined, documented and approved.	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	
2-15-2	Web Application Security	The cybersecurity requirements for external web applications must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance &	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for	5	
2-15-2	Web Application Security	The cybersecurity requirements for external web applications must be implemented.	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	
2-15-3	Web Application Security	The cybersecurity requirements for external web applications 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	
2-15-3-1	Web Application Security	Use of web application firewall.	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	8	
2-15-3-2	Web Application Security	Adoption of the multi-tier architecture principle.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or	8	
2-15-3-2	Web Application Security	Adoption of the multi-tier architecture principle.	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	
2-15-3-3	Web Application Security	Use of secure protocols (e.g., HTTPS).	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
2-15-3-3	Web Application Security	Use of secure protocols (e.g., HTTPS).	Functional	Intersects With	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	8	
2-15-3-4	Web Application Security	Clarification of the secure usage policy for users.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
2-15-3-4	Web Application Security	Clarification of the secure usage policy for users.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to	8	
2-15-3-4	Web Application Security	Clarification of the secure usage policy for users.	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.	8	
2-15-3-5	Web Application Security	Multi-factor authentication for users' access	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS);	8	
2-15-3-5	Web Application Security	Multi-factor authentication for users' access	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.	8	
2-15-4	Web Application Security	The cybersecurity requirements for external web applications must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
2-15-4	Web Application Security	The cybersecurity requirements for external web applications must be reviewed periodically.	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	
3	Cybersecurity Resilience	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3-1	Cybersecurity Resilience	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3-1-1	Cybersecurity Resilience	Cybersecurity requirements for business continuity management must be defined, documented and approved.	Functional	Subset Of	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	10	
3-1-2	Cybersecurity Resilience	The cybersecurity requirements for business continuity management must be implemented.	Functional	Intersects With	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	8	
3-1-2	Cybersecurity Resilience	The cybersecurity requirements for business continuity management must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
3-1-3	Cybersecurity Resilience	The cybersecurity requirements for business continuity management must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
3-1-3-1	Cybersecurity Resilience	Ensuring the continuity of cybersecurity systems and procedures.	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	
3-1-3-2	Cybersecurity Resilience	Developing response plans for cybersecurity incidents that may affect the business continuity.	Functional	Intersects With	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	8	
3-1-3-2	Cybersecurity Resilience	Developing response plans for cybersecurity incidents that may affect the business continuity.	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
3-1-3-2	Cybersecurity Resilience	Developing response plans for cybersecurity incidents that may affect the business continuity.	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
3-1-3-3	Cybersecurity Resilience	Developing disaster recovery plans.	Functional	Intersects With	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	8	
3-1-4	Cybersecurity Resilience	The cybersecurity requirements for business continuity management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3-1-4	Cybersecurity Resilience	The cybersecurity requirements for business continuity management must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
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	Cybersecurity requirements for contracts and agreements with third-parties must be identified, documented and approved.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4-1-2	Third-Party Cybersecurity	The cybersecurity requirements for contracts and agreements with third-parties (e.g., Service Level Agreement (SLA)) -which may affect, if impacted, the organization's data or services- must include at least the	Functional	No Relationship	N/A	N/A	N/A	0	
4-1-2-1	Third-Party Cybersecurity	Non-disclosure clauses and secure removal of organization's data by third parties upon end of service.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect	8	
4-1-2-1	Third-Party Cybersecurity	Non-disclosure clauses and secure removal of organization's data by third parties upon end of service.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties,	10	
4-1-2-2	Third-Party Cybersecurity	Communication procedures in case of cybersecurity incidents.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
4-1-2-2	Third-Party Cybersecurity	Communication procedures in case of cybersecurity incidents.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security,	5	
4-1-2-2	Third-Party Cybersecurity	Communication procedures in case of cybersecurity incidents.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
4-1-2-3	Third-Party Cybersecurity	Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
4-1-2-3	Third-Party Cybersecurity	Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
4-1-3	Third-Party Cybersecurity	The cybersecurity requirements for contracts and agreements with IT outsourcing and managed services third-parties must include at least the following:	Functional	No Relationship	N/A	N/A	N/A	0	
4-1-3-1	Third-Party Cybersecurity	Conducting a cybersecurity risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related regulatory requirements.	Functional	Subset Of	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	10	
4-1-3-1	Third-Party Cybersecurity	Conducting a cybersecurity risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related 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).	8	
4-1-3-2	Third-Party Cybersecurity	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	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.	5	
4-1-3-2	Third-Party Cybersecurity	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	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	
4-1-3-2	Third-Party Cybersecurity	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	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	
4-1-3-2	Third-Party Cybersecurity	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	Functional	Intersects With	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	8	
4-1-3-2	Third-Party Cybersecurity	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4-1-4	Third-Party Cybersecurity	The cybersecurity requirements for contracts and agreements with third-parties must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
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	Cybersecurity requirements related to the use of hosting and cloud computing services must be defined, documented and approved.	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	
4-2-2	Cloud Computing and Hosting Cybersecurity	The cybersecurity requirements related to the use of hosting and cloud computing services must be implemented.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
4-2-2	Cloud Computing and Hosting Cybersecurity	The cybersecurity requirements related to the use of hosting and cloud computing services must be implemented.	Functional	Intersects With	Operationalizing Security, Compliance &	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for	5	
4-2-3	Cloud Computing and Hosting Cybersecurity	In line with related and applicable laws and regulations, and in addition to the applicable ECC controls from main domains (1), (2), (3) and subdomain (4-1), the cybersecurity requirements related to the use of	Functional	No Relationship	N/A	N/A	N/A	0	
4-2-3-1	Cloud Computing and Hosting Cybersecurity	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.	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 with industry practices.	10	
4-2-3-1	Cloud Computing and Hosting Cybersecurity	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	8	
4-2-3-1	Cloud Computing and Hosting Cybersecurity	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	8	
4-2-3-1	Cloud Computing and Hosting Cybersecurity	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.	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	
4-2-3-2	Cloud Computing and Hosting Cybersecurity	Separation of organization's environments (specifically virtual servers) from other environments hosted at the cloud service provider.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
4-2-3-2	Cloud Computing and Hosting Cybersecurity	Separation of organization's environments (specifically virtual servers) from other environments hosted at the cloud service provider.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
4-2-3-3	Cloud Computing and Hosting Cybersecurity	Organization's information hosting and storage must be inside the Kingdom of Saudi Arabia.	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 with industry practices.	10	

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

Focal Document: Saudi Arabia - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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
4-2-3-3	Cloud Computing and Hosting Cybersecurity	Organization's information hosting and storage must be inside the Kingdom of Saudi Arabia.	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	5	
4-2-3-3	Cloud Computing and Hosting Cybersecurity	Organization's information hosting and storage must be inside the Kingdom of Saudi Arabia.	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.	5	
4-2-4	Cloud Computing and Hosting Cybersecurity	TThe cybersecurity requirements related to the use of hosting and cloud computing services must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	5	
5	Industrial Control Systems Cybersecurity	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5-1	Industrial Control Systems (ICS) Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
5-1-1	Industrial Control Systems (ICS) Protection	Cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be defined, documented and approved.	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
5-1-2	Industrial Control Systems (ICS) Protection	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be implemented.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	5	
5-1-2	Industrial Control Systems (ICS) Protection	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be implemented.	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	5	
5-1-3	Industrial Control Systems (ICS) Protection	In addition to the applicable ECC controls from the main domains (1), (2), (3) and (4), the cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must include at least the	Functional	No Relationship	N/A	N/A	N/A	0	
5-1-3-1	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
5-1-3-1	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).	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	
5-1-3-1	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).	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	
5-1-3-2	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, wireless, remote access).	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
5-1-3-2	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, wireless, remote access).	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	
5-1-3-2	Industrial Control Systems (ICS) Protection	Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, wireless, remote access).	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	
5-1-3-3	Industrial Control Systems (ICS) Protection	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	8	
5-1-3-3	Industrial Control Systems (ICS) Protection	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.	Functional	Intersects With	Power Level Monitoring	EMB-09	Automated mechanisms exist to monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering.	5	
5-1-3-3	Industrial Control Systems (ICS) Protection	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
5-1-3-3	Industrial Control Systems (ICS) Protection	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.	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	
5-1-3-4	Industrial Control Systems (ICS) Protection	Isolation of Safety Instrumental Systems (SIS).	Functional	Intersects With	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	8	
5-1-3-5	Industrial Control Systems (ICS) Protection	Strict limitation on the use of external storage media.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS)	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
5-1-3-5	Industrial Control Systems (ICS) Protection	Strict limitation on the use of external storage media.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	8	
5-1-3-5	Industrial Control Systems (ICS) Protection	Strict limitation on the use of external storage media.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	8	
5-1-3-6	Industrial Control Systems (ICS) Protection	Strict limitation on connecting mobile devices to industrial production networks.	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.	8	
5-1-3-6	Industrial Control Systems (ICS) Protection	Strict limitation on connecting mobile devices to industrial production networks.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	8	
5-1-3-6	Industrial Control Systems (ICS) Protection	Strict limitation on connecting mobile devices to industrial production networks.	Functional	Intersects With	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	8	
5-1-3-7	Industrial Control Systems (ICS) Protection	Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices.	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	
5-1-3-7	Industrial Control Systems (ICS) Protection	Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices.	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	8	
5-1-3-7	Industrial Control Systems (ICS) Protection	Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices.	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	8	
5-1-3-8	Industrial Control Systems (ICS) Protection	Vulnerability management for industrial control systems and operational technology (ICS/OT).	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
5-1-3-8	Industrial Control Systems (ICS) Protection	Vulnerability management for industrial control systems and operational technology (ICS/OT).	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
5-1-3-8	Industrial Control Systems (ICS) Protection	Vulnerability management for industrial control systems and operational technology (ICS/OT).	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
5-1-3-9	Industrial Control Systems (ICS) Protection	Patch management for industrial control systems and operational technology (ICS/OT).	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.	5	
5-1-3-10	Industrial Control Systems (ICS) Protection	Cybersecurity applications management related to the protection of the industrial systems from viruses and malware.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
5-1-4	Industrial Control Systems (ICS) Protection	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be reviewed periodically.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
5-1-4	Industrial Control Systems (ICS) Protection	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be reviewed periodically.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their	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 - Essential Cybersecurity Controls (ECC – 1 : 2018)
Focal Document URL: https://nca.gov.sa/ar/ecc-en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-ecc-1-2018.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