NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **UAE National Information Assurance Framework (NIAF)**
Focal Document URL: https://u.ae/-/media/Documents-2023/National-Information-Assurance-Framework-NIAF.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-emea-uae-niaf.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1	Risk Assessment	Risk assessment is the central component of an effective life cycle approach to IA, helping to identify the highest risk areas and assisting IA (or information security) managers with the prioritizing and allocation of resources to efficiently reduce overall risk. This requires a systematic and repeatable approach for assessing the posture of cybersecurity systems and networks, enabling expenditures on controls to be balanced against the potential harm of security failures. The risk assessment methodology outlined here ensures a uniform approach across all entities and produces comparable results, while still offering each entity the freedom needed to leverage its existing processes and meet its own business needs. The National Cyber Security Risk Management Framework provides further detailed description and guidance to critical entities on the appropriate approach and methodology to conduct risk assessment.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.1	Asset Inventory	Each entity must have a clear understanding of the types of information assets (e.g. hardware, software, databases) under its ownership and/or control, for as-is and to-be enterprise architectures.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
3.1.2	Business Impact Analysis	Each entity must evaluate the potential impact in case of a security breach or service interruption of its own information assets, including developing a clear understanding of which activities, processes, and functions each individual information asset supports.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
3.1.3	Vulnerability Assessment	Each entity must evaluate the threat exposure levels of their key information assets and the likelihood of an assault upon exploiting those vulnerabilities.	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.2	Integrated Security	Based on the results of the risk assessment, the individual entities must document how identified risks will be mitigated. As a minimum, this includes clearly identifying an integrated set of logical, physical, and personnel security controls to be implemented and the underlying rationale for a control selection based on a cost-benefit analysis.	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
3.2.1	Logical Security	Each entity must define the appropriate logical security controls (e.g. firewalls, encryption, anti-virus, identity management, etc.) required to protect the information assets under its control and or ownership.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
3.2.1	Logical Security	Each entity must define the appropriate logical security controls (e.g. firewalls, encryption, anti-virus, identity management, etc.) required to protect the information assets under its control and or ownership.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
3.2.2	Physical Security	Each entity must define the physical security controls (e.g. door locks, perimeter fence, fire alarms, etc.) required to protect the information assets under its control and or ownership.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.2.2	Physical Security	Each entity must define the physical security controls (e.g. door locks, perimeter fence, fire alarms, etc.) required to protect the information assets under its control and or ownership.	Functional	intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.2.3	Personnel Security	Each entity must define the personnel security controls (e.g. background checks, post-employment return of assets, etc.) required to protect the information assets under its control and or ownership.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
3.2.3	Personnel Security	Each entity must define the personnel security controls (e.g. background checks, post-employment return of assets, etc.) required to protect the information assets under its control and or ownership.	Functional	intersects with	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
3.3	Incident Management	To minimize the impact of cybersecurity incidents, each entity must have the capacity to monitor its own information assets, identify and manage cybersecurity incidents, and escalate incidents to a sector or national level taking into account and utilizing as appropriate the National Incident Management Capability established by NESA.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
3.3.1	Situational Awareness	Each entity must possess the internal capacity to monitor the constant state of its own information assets and an overall awareness of its surrounding environment. This includes the ability to detect internal cybersecurity incidents, and taking into account any threat, warning, or incident-related information received from external sources.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.3.1	Situational Awareness	Each entity must possess the internal capacity to monitor the constant state of its own information assets and an overall awareness of its surrounding environment. This includes the ability to detect internal cybersecurity incidents, and taking into account any threat, warning, or incident-related information received from external sources.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
3.3.2	Entity Incident Response	Each entity must develop an internal incident response capability that minimizes the impact of internal incidents or incidents arising from other entities that could affect them directly or indirectly. The national framework for cybersecurity incident management, as well as other NESA's issuances, define these minimum capabilities to be put in place by the critical entities.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
3.3.2	Entity Incident Response	Each entity must develop an internal incident response capability that minimizes the impact of internal incidents or incidents arising from other entities that could affect them directly or indirectly. The national framework for cybersecurity incident management, as well as other NESA's issuances, define these minimum capabilities to be put in place by the critical entities.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.3.3	Escalation to Sector and National Levels	Each entity must have the processes and communication channels in place to escalate a significant incident to the sector level and to the national level, in accordance with the national framework for cybersecurity incident management developed by NESA.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.3.3	Escalation to Sector and National Levels	Each entity must have the processes and communication channels in place to escalate a significant incident to the sector level and to the national level, in accordance with the national framework for cybersecurity incident management developed by NESA.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
3.4	Business Continuity	As a result of the business impact analysis, each entity should identify which information assets are the most crucial to the normal functioning of business. Each entity must ensure that these critical business functions will be available to customers, suppliers, and other actors as needed, including during significant cybersecurity events or other incidents (e.g. natural disasters) that might impact availability of these critical information assets. Business continuity is not only implemented at the time of a disaster but requires the performance of daily activities to maintain service, consistency, and recoverability.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.4	Business Continuity	As a result of the business impact analysis, each entity should identify which information assets are the most crucial to the normal functioning of business. Each entity must ensure that these critical business functions will be available to customers, suppliers, and other actors as needed, including during significant cybersecurity events or other incidents (e.g. natural disasters) that might impact availability of these critical information assets. Business continuity is not only implemented at the time of a disaster but requires the performance of daily activities to maintain service, consistency, and recoverability.	Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
3.4.1	Continuity Planning	Prior to the occurrence of a disastrous incident, each entity must have developed and regularly tested a plan for continuing critical services and operations under significantly adverse conditions that may impact its critical information assets.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.4.1	Continuity Planning	Prior to the occurrence of a disastrous incident, each entity must have developed and regularly tested a plan for continuing critical services and operations under significantly adverse conditions that may impact its critical information assets.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
3.4.2	Disaster Recovery	Each entity must have an internal disaster recovery plan that illustrates the process of rapid recovery of critical information assets during a catastrophic interruption.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.4.2	Disaster Recovery	Each entity must have an internal disaster recovery plan that illustrates the process of rapid recovery of critical information assets during a catastrophic interruption.	Functional	intersects with	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
3.4.3	Return to Steady State	Each entity must define a business resumption plan that ensures the smooth transition of critical information assets back to a state of normal service following a disruption.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.4.3	Return to Steady State	Each entity must define a business resumption plan that ensures the smooth transition of critical information assets back to a state of normal service following a disruption.	Functional	intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	