NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/39/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-39.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	FRAMING RISK	See fDE for details.	Functional	Subset Of	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	10	
TASK 1-1	RISK ASSUMPTIONS	Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
TASK 1-2	RISK CONSTRAINTS	Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
TASK 1-3	RISK TOLERANCE	Identify the level of risk tolerance for the organization.	Functional	Equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
TASK 1-4	PRIORITIES AND TRADE-OFFS	Identify priorities and trade-offs considered by the organization in managing risk.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
TASK 1-4	PRIORITIES AND TRADE-OFFS	Identify priorities and trade-offs considered by the organization in managing risk.	Functional	Intersects With	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
TASK 1-4	PRIORITIES AND TRADE-OFFS	Identify priorities and trade-offs considered by the organization in managing risk.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
3.2	ASSESSING RISK	See fDE for details.	Functional	Subset Of	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).	10	
TASK 2-1	THREAT AND VULNERABILITY IDENTIFICATION	Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
TASK 2-1	THREAT AND VULNERABILITY IDENTIFICATION	Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	
TASK 2-1	THREAT AND VULNERABILITY IDENTIFICATION	Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	8	
TASK 2-1	THREAT AND VULNERABILITY IDENTIFICATION	Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
TASK 2-2	RISK DETERMINATION	Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.	Functional	Subset Of	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).	10	
3.3	RESPONDING TO RISK	See fDE for details.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
3.3	RESPONDING TO RISK	See fDE for details.	Functional	Intersects With	Risk Response	RSK-06.1	remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	8	
3.3	RESPONDING TO RISK	See fDE for details.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
3.3	RESPONDING TO RISK	See fDE for details.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	5	
3.3	RESPONDING TO RISK	See fDE for details.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
TASK 3-1	RISK RESPONSE IDENTIFICATION	Identify alternative courses of action to respond to risk determined during the risk assessment.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
TASK 3-1	RISK RESPONSE IDENTIFICATION	Identify alternative courses of action to respond to risk determined during the risk assessment.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	5	
TASK 3-2	EVALUATION OF ALTERNATIVES	Evaluate alternative courses of action for responding to risk.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	5	
TASK 3-3	RISK RESPONSE DECISION	Decide on the appropriate course of action for responding to risk.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
TASK 3-4	RISK RESPONSE IMPLEMENTATION	Implement the course of action selected to respond to risk.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
TASK 3-4	RISK RESPONSE IMPLEMENTATION	Implement the course of action selected to respond to risk.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
3.4	MONITORING RISK	See fDE for details.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);	5	
TASK 4-1	RISK MONITORING STRATEGY	Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
TASK 4-2	RISK MONITORING	Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.	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	
TASK 4-2	RISK MONITORING	Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	