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 800-37 - Risk Management Framework for Information Systems and Organizations**
Focal Document URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-37-r2.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	PREPARE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK P-1	RISK MANAGEMENT ROLES	Identify and assign individuals to specific roles associated with security and privacy risk management.	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).	8	
TASK P-1	RISK MANAGEMENT ROLES	Identify and assign individuals to specific roles associated with security and privacy risk management.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
TASK P-1	RISK MANAGEMENT ROLES	Identify and assign individuals to specific roles associated with security and privacy risk management.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	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, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
TASK P-2	RISK MANAGEMENT STRATEGY	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
TASK P-3	RISK ASSESSMENT—ORGANIZATION	Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
TASK P-3	RISK ASSESSMENT—ORGANIZATION	Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.	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	
TASK P-4	ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (Optional)	Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.	Functional	Subset Of	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10	
TASK P-5	COMMON CONTROL IDENTIFICATION	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.	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	
TASK P-5	COMMON CONTROL IDENTIFICATION	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
TASK P-6	IMPACT-LEVEL PRIORITIZATION (Optional)	Prioritize organizational systems with the same impact level.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
TASK P-6	IMPACT-LEVEL PRIORITIZATION (Optional)	Prioritize organizational systems with the same impact level.	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	
TASK P-7	CONTINUOUS MONITORING STRATEGY—ORGANIZATION	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	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 P-7	CONTINUOUS MONITORING STRATEGY—ORGANIZATION	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
TASK P-8	MISSION OR BUSINESS FOCUS	Identify the missions, business functions, and mission/business processes that the system is intended to support.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
TASK P-8	MISSION OR BUSINESS FOCUS	Identify the missions, business functions, and mission/business processes that the system is intended to support.	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	
TASK P-8	MISSION OR BUSINESS FOCUS	Identify the missions, business functions, and mission/business processes that the system is intended to support.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
TASK P-8	MISSION OR BUSINESS FOCUS	Identify the missions, business functions, and mission/business processes that the system is intended to support.	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 set of protection needs is obtained.	8	
TASK P-9	SYSTEM STAKEHOLDERS	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	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	
TASK P-9	SYSTEM STAKEHOLDERS	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	8	
TASK P-9	SYSTEM STAKEHOLDERS	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	3	
TASK P-10	ASSET IDENTIFICATION	Identify assets that require protection.	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
TASK P-11	AUTHORIZATION BOUNDARY	Determine the authorization boundary of the system.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
TASK P-11	AUTHORIZATION BOUNDARY	Determine the authorization boundary of the system.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
TASK P-11	AUTHORIZATION BOUNDARY	Determine the authorization boundary of the system.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	8	
TASK P-12	INFORMATION TYPES	Identify the types of information to be processed, stored, and transmitted by the system.	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
TASK P-13	INFORMATION LIFE CYCLE	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
TASK P-13	INFORMATION LIFE CYCLE	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
TASK P-14	RISK ASSESSMENT—SYSTEM	Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
TASK P-14	RISK ASSESSMENT—SYSTEM	Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	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	
TASK P-15	REQUIREMENTS DEFINITION	Define the security and privacy requirements for the system and the environment of operation.	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	
TASK P-15	REQUIREMENTS DEFINITION	Define the security and privacy requirements for the system and the environment of operation.	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	
TASK P-16	ENTERPRISE ARCHITECTURE	Determine the placement of the system within the enterprise architecture.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
TASK P-17	REQUIREMENTS ALLOCATION	Allocate security and privacy requirements to the system and to the environment of operation.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TASK P-17	REQUIREMENTS ALLOCATION	Allocate security and privacy requirements to the system and to the environment of operation.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
TASK P-18	SYSTEM REGISTRATION	Register the system with organizational program or management offices.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
TASK P-18	SYSTEM REGISTRATION	Register the system with organizational program or management offices.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
3.2	CATEGORIZE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK C-1	SYSTEM DESCRIPTION	Document the characteristics of the system.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including	10	
TASK C-2	SECURITY CATEGORIZATION	Categorize the system and document the security categorization results.	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TASK C-3	SECURITY CATEGORIZATION REVIEW AND APPROVAL	Review and approve the security categorization results and decision.	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	
3.3	SELECT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK S-1	CONTROL SELECTION	Select the controls for the system and the environment of operation.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TASK S-2	CONTROL TAILORING	Tailor the controls selected for the system and the environment of operation.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
TASK S-2	CONTROL TAILORING	Tailor the controls selected for the system and the environment of operation.	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 S-3	CONTROL ALLOCATION	Allocate security and privacy controls to the system and to the environment of operation.	Functional	Subset Of	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TASK S-4	DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	Document the controls for the system and environment of operation in security and privacy plans.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including	10	
TASK S-5	CONTINUOUS MONITORING STRATEGY— SYSTEM	Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including	10	
TASK S-6	PLAN REVIEW AND APPROVAL	Review and approve the security and privacy plans for the system and the environment of operation.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including	10	
3.4	IMPLEMENT	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK I-1	CONTROL IMPLEMENTATION	Implement the controls in the security and privacy plans.	Functional	Subset Of	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TASK I-2	UPDATE CONTROL IMPLEMENTATION INFORMATION	Document changes to planned control implementations based on the "as-implemented" state of controls.	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);	8	
3.5	ASSESS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK A-1	ASSESSOR SELECTION	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	Functional	Subset Of	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.	10	
TASK A-1	ASSESSOR SELECTION	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	Functional	Intersects With	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	5	
TASK A-1	ASSESSOR SELECTION	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	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; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
TASK A-2	ASSESSMENT PLAN	Develop, review, and approve plans to assess implemented controls.	Functional	Subset Of	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.	10	
TASK A-3	CONTROL ASSESSMENTS	Assess the controls in accordance with the assessment procedures described in assessment plans.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are: (1) Implemented correctly; and (2) Operating as intended.	8	
TASK A-3	CONTROL ASSESSMENTS	Assess the controls in accordance with the assessment procedures described in assessment plans.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
TASK A-4	ASSESSMENT REPORTS	Prepare the assessment reports documenting the findings and recommendations from the control assessments.	Functional	Subset Of	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	10	
TASK A-5	REMEDIATION ACTIONS	Conduct initial remediation actions on the controls and reassess remediated controls.	Functional	Subset Of	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.	10	
TASK A-5	REMEDIATION ACTIONS	Conduct initial remediation actions on the controls and reassess remediated controls.	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 A-6	PLAN OF ACTION AND MILESTONES	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.	Functional	Subset Of	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);	10	
3.6	AUTHORIZE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK R-1	AUTHORIZATION PACKAGE	Assemble the authorization package and submit the package to the authorizing official for an authorization decision.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
TASK R-2	RISK ANALYSIS AND DETERMINATION	Analyze and determine the risk from the operation or use of the system or the provision of common controls.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
TASK R-3	RISK RESPONSE	Identify and implement a preferred course of action in response to the risk determined.	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 R-3	RISK RESPONSE	Identify and implement a preferred course of action in response to the risk determined.	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 R-4	AUTHORIZATION DECISION	Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	8	
TASK R-4	AUTHORIZATION DECISION	Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
TASK R-5	AUTHORIZATION REPORTING	Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
3.7	MONITOR	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TASK M-1	SYSTEM AND ENVIRONMENT CHANGES	Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	Functional	Subset Of	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	10	
TASK M-2	ONGOING ASSESSMENTS	Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are: (1) Implemented correctly; and (2) Operating as intended.	5	
TASK M-3	ONGOING RISK RESPONSE	Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	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.	5	
TASK M-4	AUTHORIZATION PACKAGE UPDATES	Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
TASK M-5	SECURITY AND PRIVACY REPORTING	Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
TASK M-6	ONGOING AUTHORIZATION	Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
TASK M-7	SYSTEM DISPOSAL	Implement a system disposal strategy and execute required actions when a system is removed from operation.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
TASK M-7	SYSTEM DISPOSAL	Implement a system disposal strategy and execute required actions when a system is removed from operation.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	