Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.2
Focal Document: DoD Zero Trust Reference Architecture v2 (July 2022)
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-2-dod-zta-reference-architecture-2-0.pdf

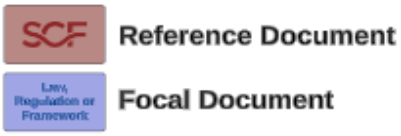
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

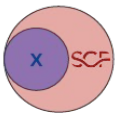
Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**

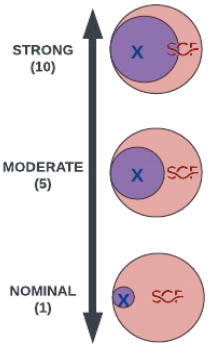


Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

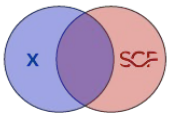


SUBSET OF
Relative Relationship Strength (control versus control)

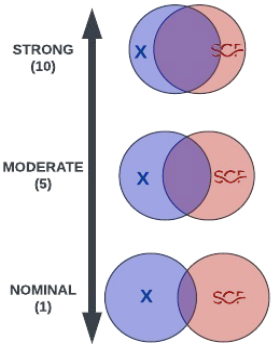


Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

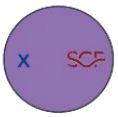


INTERSECTS WITH
Relative Relationship Strength (control versus control)

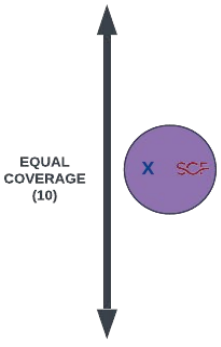


Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

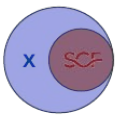


EQUAL
Relative Relationship Strength (control versus control)

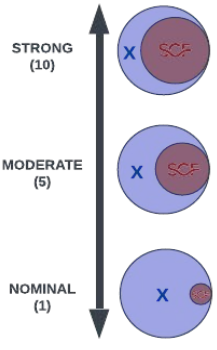


Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

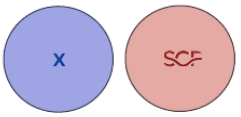


SUPERSET OF
Relative Relationship Strength (control versus control)

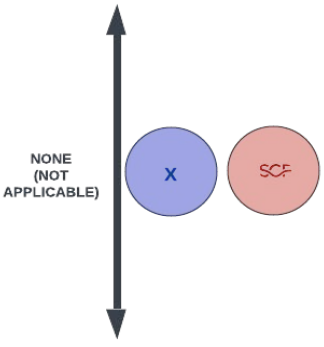


Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.



NO RELATIONSHIP
Relative Relationship Strength (control versus control)



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)
1.0	Continuous Authentication	The ability validate network users are the ones who they claim to be throughout an entire session at every step.	Functional	equal	Continuous Authentication	IAC-13.3	Automated mechanisms exist to enable continuous re-authentication through the lifecycle of entity interactions.	10	
1.1	Continuous Multifactor Authentication	The ability to conduct authentication using two or more different factors to achieve authentication. Factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric), something you do. Continuous means just-in-time authentication (just -in time usually refers to authorization).	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: • Remote network access; • Third-party systems, applications and/or services; and/ or • Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
1.2	Behavioral Biometrics	Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
			Functional	intersects with	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
2.0	Conditional Authorization (Users, NPEs, M2M)	The ability to grant authorization to a resource contingent upon the continued trustworthiness of the supplicant. This trustworthiness can affect by the device hygiene, user and entity behavior, and other factors.	Functional	intersects with	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.	2	
2.1	Attribute-Based Access Control (ABAC)	An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
2.2	Device Hygiene	The ability to determine the compliance status of managed and unmanaged assets.	Functional	intersects with	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational technology assets.	5	
2.2.1	Continuous, automated, Inventory & Telemetry	The ability to locate and identify devices connected to an environment, detect their removal/addition, to accurately know the totality of assets that need to be monitored and protected within the enterprise, and to obtain information about them. [CIS] Also support identifying unauthorized and unmanaged assets to remove or remediate.	Functional	intersects with	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
			Functional	intersects with	Dynamic Host Configuration Protocol (DHCP) Server Logging	AST-02.6	Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems.	5	
			Functional	intersects with	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
2.2.2	Status Scans & Dynamic Instrumentation	The ability to poll devices for status, state, and configuration via remote management function or installation of agents/code on the device bymanagement.	Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
			Functional	intersects with	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
2.2.3	Dynamic Device Service Updates	The ability to remotely install new configurations and services on a device in order to bring the device into conformity or compliance with existing policy.	Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
2.3	Just in Time Authorization	Just in Time Authorization allows a timed expiration of group membership. In practice, this allows administrative rights to be given at the time of need for as long as an action or duty needs them. As a result, access to administrative privileges becomes limited and abuse must be timed for when those privileges are given.	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
2.4	Privileged Access Management	Privileged Access Management (PAM) refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets.	Functional	equal	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	
3.0	ZT enabling Infrastructure	Infrastructure capabilities that enable ZT	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	
			Functional	intersects with	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
			Functional	intersects with	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.	5	
			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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
			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 correctness of higher layers.	5	
3.1	Macro-segmentation	Similar in concept to physical network segmentation, macro-segmentation can be achieved through the application of additional hardware or VLANs.	Functional	equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
3.2	Micro-segmentation	Micro-segmentation is the practice of dividing (isolating) the network into small logical segments by enabling granular access control, whereby users, applications, workloads and devices are segmented based on logical, not physical, attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious actors). In a ZT Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.	Functional	equal	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	10	
3.2.1	Workload Definition	The ability to define the objectives, compute requirements, and communication pathways required for a specific application workload.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	2	
3.2.2	Workload Isolation	The ability to segment out an application workload so as to only allow the required connections be made between processes, network traffic, and api calls. As a subset of micro-segmentation the capability is limiting east west traffic preventing lateral movement.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.3	Software-defined perimeter (SDP)	The ability to control access to resources based on identity and a need-to-know model in which device state and identity are verified before access to application infrastructure is granted.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.0	Securing Application & Workload	The ability to secure and manage the application layer as well as compute containers and virtual machines. The ability to identify and control the technology stack to facilitate more granular and accurate access decisions.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.1	API and Process Micro Segmentation	The ability to allow or block communication of API calls and process to process communication on both remote and local systems.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.2	Securing Software Supply Chain	The ability to prevent or arrest software supply chain attacks, which occur "when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers."	Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
			Functional	intersects with	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
			Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	intersects with	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.	5	
			Functional	intersects with	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of systems, applications and services.	5	
4.2.1	DevSecOps	A process capability that improves the lead time and frequency of delivery outcomes through enhanced engineering practices; promoting a more cohesive collaboration between Development, Security, and Operations teams as they work towards continuous integration and delivery.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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)
4.2.2	API Standardization	The ability to reach agreement and publish, locally, the applicatoin programming interface for a commonly used service. Enforecement ofcompliance in the use of commonly agreed API's.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.3	Application Proxies	An application proxy or application proxy server receives requests intended for another server and acts as the proxy of the client to obtain the requested service.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.4	Risk-adaptive Application Access	In Risk-adaptive Application Access, access privileges are granted based on a combination of a user's identity, mission need, and the level of security risk that exists between the system being accessed and a user. RAdAC will use security metrics, such as the strength of the authentication method, the level of assurance of the session connection between the system and a user, and the physical location of a user, to make its risk determination.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.0	Securing Data	Processes and technical controls to identify, classify, securely handle, retain, and dispose of data.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
			Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	intersects with	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
			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	
5.1	Encryption	A procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data.	Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
5.1.1	Encryption In Transit	The ability to protect data if communications are intercepted while data moves between sites or services. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival.	Functional	equal	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
5.1.2	Encryption At Rest	The ability to protect data from a system compromise or data exfiltration by encrypting data while stored.	Functional	equal	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	10	
5.2	Dynamic Policy enforcement	The ability to adapt policy and configurations, and enforce that change, in near real time based on environmental circumstances and indications of user and network behavior.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.3	Data Rights Management (DRM)	DRM is a set of access control technologies and policies that proactively detect and protect access to data and proprietary hardware and prevent unauthorized modification or redistribution of protected data.	Functional	equal	Data Rights Management (DRM)	DCH-27	Automated mechanisms exist to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	10	
5.4	Data Loss Prevention (DLP)	The ability to detect and prevent the unauthorized use and transmission of information.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
5.5	Dynamic Data Masking	The ability to provide a column-level security feature that uses masking policies to selectively mask tables and columns at query time.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.6	Data Discovery & Classification	The ability to discover, classify, label, and report upon the sensitive data in your databases.	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	
5.6.1	Data Tagging	The ability to associate a data object with characterizing metadata for a defined purpose.	Functional	intersects with	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
6.0	Analytics	The ability to systematically apply statistical and /or logical techniques to describe and illustrate, condense, and recap, and evaluate data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.1	Data Visualization	The ability to represent information graphically, highlighting patterns and trends in data and helping the reader to achieve quick insights.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.2	Security Information and Event Management (SIEM)	The ability to centrally collect event and incident alerts across disparate sources, analyze them, and provide reports, situational awareness, and notifications. It is frequently used in support of incidence response, compliance, and reporting.	Functional	equal	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.	10	
6.3	Big Data	The ability to enable enhanced insight, decision making, and process automation by consuming high- volume, high-velocity and/or high-variety information assets.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.4	Sensors & Telemetry	The ability to collect status, state, and configuration of a service or device via the use of active or passive probes or other analytic activities on the device.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.5	Continuous Monitoring	The ability to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
6.6	Machine Learning	The ability to apply machine learning algorithms composed of many technologies (such as deep learning, neural networks and natural language processing), in unsupervised and supervised learning, that operate guided by lessons from existing information.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.7	Entity and Activity Auditing	The ability to conduct "Monitoring for anomalous or suspicious behavior …with signatures, statistical analysis, analytics or machine learning on user activity events. The analysis seeks to find patterns amongst data generated by user activity.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
7.0	ZT Governance	A set of processes that ensures that ZT assets are formally managed throughout the enterprise. A ZT governance model establishes authority and management and decision making parameters related to ZT policies produced or managed by the enterprise.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.0	ZT Orchestration	The ability to coordinate and automate disparate Zero Trust services, systems, and activities as part of of Cybersecurity Domain Orchestrator.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1	Automation	The ability to create and apply application technology to monitor and control the production and delivery of otherwise manual services.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1.1	Artificial Intelligence	The capability of computer processes to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1.2	Robotic Process Automation	The ability to use software tools that partially or fully automate human activities that are manual, rule- based, and repetitive.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1.3	Policy Administrator	A component with the ability to establish and/or shut down the communication path between a subject and a resource (via commands to relevant Policy Enforcement Points). The ability to direct Policy Enforcement Points to grant or deny access to resources based on policies created by the policy engine.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.2	ZT Policy Engine	The ability for a component responsible for the ultimate decision to grant access to a resource for a given subject.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.3	ZT Policy Administration	The ability to coordinate and enforce policy created by the ZT policy engine by translating it to settings and configurations at designated policy enforcementpoints (PEPs).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4	Software-Defined Enterprise	The ability to create a virtualized layer over physical infrastructure, and centrally manage it in an automated manner, utilizing a policy-based access control to dynamically create, configure, provision, and decommission virtualized network functions, system functions, security functions, and workflows.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4.1	Domain Orchestration	The ability to coordinate services and operations, for a specific domain, across multiple types of devices and systems.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4.2	Domain Control	The ability direct or command elements and associated systems to perform specific actions within a specified domain.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4.3	Software Defined Networking	The ability to separate the control and data planes and centrally manage and control the elements in the data plane.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4.5	Software-defined Wide-area Network	The ability to virtualizethe enterprise connection of local networks into a wide-area network through the use of central routing, management, control & configuration ofvirtualized, distributed network and security services.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.4.6	Network Function Virtualization / Virtual Security Function	The ability to decouple network functions (VNF) and security functions (VSF) from hardware appliances anddeliver those functions as software in virtual machines.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.5	Data Governance	A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision making parameters related to the data produced or managed by theenterprise.	Functional	equal	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	10	
8.6	Risk Management Framework	Provides a comprehensive, flexible, repeatable, and measurable process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs tomeet the requirements of the Federal Information Security Modernization Act (FISMA).	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	