Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.4**
Focal Document: **NIST SP 800-171 R2**
Focal Document URL: **https://csrc.nist.gov/pubs/sp/800/171/r2/final**
STRM URL: **https://securecontrolsframework.com/content/strm/scf-strm-nist-800-171-r2.pdf**

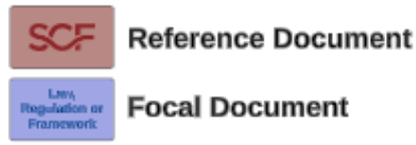
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

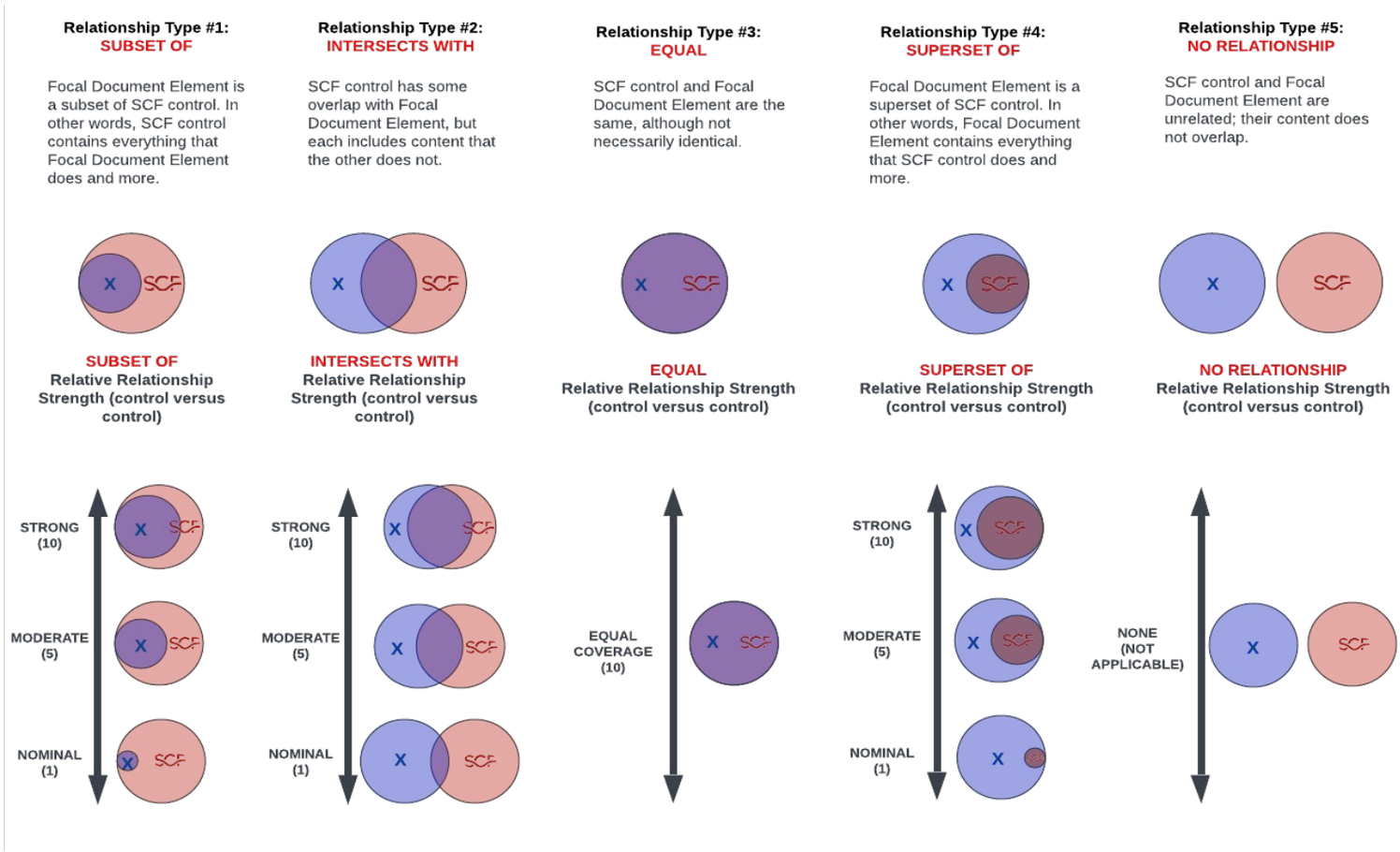
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

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**





FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
			intersects with	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
			equal	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	
			intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
			intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Functional	intersects with	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
			intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
			intersects with	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	5	
			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	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Functional	equal	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
			equal	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	10	
			intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
			intersects with	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	5	
			intersects with	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.	5	
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	Functional	equal	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Functional	intersects with	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	5	
			equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	10	
3.1.8	Limit unsuccessful logon attempts.	Functional	equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Functional	equal	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides cybersecurity & data privacy notices.	10	
			intersects with	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system that provides cybersecurity & data privacy notices.	5	
			intersects with	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized source, such as Active Directory.	5	
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Functional	equal	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	10	
			intersects with	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.	5	
3.1.11	Terminate (automatically) a user session after a defined condition.	Functional	equal	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10	
3.1.12	Monitor and control remote access sessions.	Functional	intersects with	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
3.1.12	Monitor and control remote access sessions.	Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
			intersects with	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to systems and data for remote workers.	5	
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Functional	equal	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10	
3.1.14	Route remote access via managed access control points.	Functional	equal	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	Functional	equal	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10	
3.1.16	Authorize wireless access prior to allowing such connections.	Functional	equal	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
3.1.17	Protect wireless access using authentication and encryption.	Functional	intersects with	Authentication & Encryption	NET-15.1	Mechanisms exist to protect wireless access through authentication and strong encryption.	5	
3.1.18	Control connection of mobile devices.	Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
			equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems.	10	
			intersects with	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.	5	
			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.	5	
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	Functional	equal	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.	10	
			equal	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	10	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.20	Verify and control/limit connections to and use of external systems.	Functional	intersects with	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external systems or service.	5	
3.1.21	Limit use of portable storage devices on external systems.	Functional	equal	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	10	
3.1.22	Control CUI posted or processed on publicly accessible systems.	Functional	intersects with	Sensitive Data In Public Cloud Providers	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
			intersects with	Publicly Accessible Content	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
			intersects with	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
			intersects with	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
			intersects with	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Functional	equal	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Functional	equal	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Functional	equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Functional	equal	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	10	
			equal	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 and contractual retention requirements.	10	
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Functional	equal	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
3.3.3	Review and update logged events.	Functional	equal	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
			intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
3.3.4	Alert in the event of an audit logging process failure.	Functional	equal	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
			equal	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10	
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Functional	equal	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	10	
			intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Functional	equal	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	
			intersects with	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
			intersects with	Sensitive Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
			equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
			equal	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	10	
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	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	
			intersects with	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.	5	
			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	
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Functional	equal	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.	10	
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
			equal	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
3.4.4	Analyze the security impact of changes prior to implementation.	Functional	equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Functional	equal	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	10	
			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 systems.	5	
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Functional	equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Functional	equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	
			intersects with	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Functional	equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
3.4.9	Control and monitor user-installed software.	Functional	equal	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	10	
			intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
3.5.1	Identify system users, processes acting on behalf of users, and devices.	Functional	equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
			intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
			intersects with	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
			intersects with	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
			intersects with	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	Functional	equal	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	
3.5.5	Prevent reuse of identifiers for a defined period.	Functional	equal	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	10	
3.5.6	Disable identifiers after a defined period of inactivity.	Functional	intersects with	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Functional	equal	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
3.5.8	Prohibit password reuse for a specified number of generations.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
3.5.10	Store and transmit only cryptographically-protected passwords.	Functional	intersects with	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
3.5.11	Obscure feedback of authentication information.	Functional	equal	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10	
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Functional	equal	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	
			intersects with	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Functional	equal	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	
3.6.3	Test the organizational incident response capability.	Functional	equal	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	10	
3.7.1	Perform maintenance on organizational systems.	Functional	equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	10	
			intersects with	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	5	
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Functional	equal	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	10	
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Functional	equal	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Functional	equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Functional	equal	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	10	
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	Functional	equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			intersects with	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
3.8.2	Limit access to CUI on system media to authorized users.	Functional	equal	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	10	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	Functional	equal	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
3.8.4	Mark media with necessary CUI markings and distribution limitations.	Functional	equal	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.	10	
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Functional	equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Functional	equal	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	10	
3.8.7	Control the use of removable media on system components.	Functional	equal	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	10	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Functional	equal	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	10	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			intersects with	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	Functional	equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
			intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Functional	equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
			intersects with	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
			intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
			intersects with	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
			intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
			intersects with	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
			intersects with	Monitoring Physical Access To Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	5	
3.10.3	Escort visitors and monitor visitor activity.	Functional	intersects with	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
			intersects with	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
3.10.4	Maintain audit logs of physical access.	Functional	equal	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
3.10.5	Control and manage physical access devices.	Functional	equal	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).	10	
			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.	5	
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	Functional	intersects with	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to systems and data for remote workers.	5	
			equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Functional	equal	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 systems and data.	10	
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Functional	equal	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	
			intersects with	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	5	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	Functional	equal	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	10	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Functional	equal	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	10	
			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.	5	
			intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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	
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Functional	equal	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.	10	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Functional	equal	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	10	
			intersects with	Threat Intelligence Feeds 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, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Functional	equal	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	10	
			intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Functional	equal	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Functional	intersects with	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
			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	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	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	
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Functional	equal	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	10	
3.13.13	Control and monitor the use of mobile code.	Functional	equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
3.13.15	Protect the authenticity of communications sessions.	Functional	equal	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
3.13.16	Protect the confidentiality of CUI at rest.	Functional	equal	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	10	
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Functional	intersects with	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
			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	
			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	
3.13.3	Separate user functionality from system management functionality.	Functional	equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Functional	equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Functional	intersects with	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.	5	
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Functional	equal	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	10	
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Functional	equal	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	10	
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Functional	equal	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	10	
			intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Functional	equal	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	10	
3.14.1	Identify, report, and correct system flaws in a timely manner.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	Functional	equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
3.14.3	Monitor system security alerts and advisories and take action in response.	Functional	equal	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
			subset of	Threat Intelligence Feeds 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, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			intersects with	Threat Intelligence Feeds 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	
3.14.4	Update malicious code protection mechanisms when new releases are available.	Functional	equal	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	10	
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Functional	equal	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	10	
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Functional	equal	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10	
			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	
3.14.7	Identify unauthorized use of organizational systems.	Functional	equal	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - AC-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - AT-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - AT-4	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].	Functional	intersects with	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-system training.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - AU-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency].	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-2(1)	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.	Functional	intersects with	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity & data privacy control assessments.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-3	The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].	Functional	intersects with	System Interconnections	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection, the interface characteristics, cybersecurity & data privacy requirements and the nature of the information communicated.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-3(5)	The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.	Functional	intersects with	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-7(1)	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CA-9	The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	Functional	intersects with	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CM-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CM-2(1)	The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.	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 (3) As part of system component installations and upgrades.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - CM-2(7)	The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.	Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CM-3(2)	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CM-8(5)	The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	Functional	intersects with	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
		Functional	intersects with	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - IA-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency].	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - IR-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - IR-8	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.	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.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - MA-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency].	Functional	subset of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - MA-4(2)	The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	Functional	intersects with	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - MP-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and	Functional	intersects with	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - PE-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PE-16	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	Functional	intersects with	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PE-6(1)	The organization monitors physical intrusion alarms and surveillance equipment.	Functional	intersects with	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PE-8	The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].	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.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PL-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
		Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PL-2(3)	The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.	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.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PL-4	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information	Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PL-4(1)	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PL-8	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO – PL-8	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PS-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency].	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PS-6	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].	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.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - PS-7	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance.	Functional	intersects with	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity & data privacy roles and responsibilities.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - PS-8	The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - RA-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - RA-5(1)	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Functional	intersects with	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - RA-5(2)	The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	Functional	intersects with	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].	Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-10	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	Functional	intersects with	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-11	The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-2	The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-3	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-4	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements;	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - SA-4	b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
			intersects with	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by the third-party.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-4(1)	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Functional	intersects with	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the controls.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-4(10)	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	Functional	intersects with	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-4(2)	The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].	Functional	intersects with	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the controls.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-4(9)	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Functional	intersects with	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-5	The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].	Functional	intersects with	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-9	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.	Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SA-9(2)	The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.	Functional	intersects with	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its processes and technologies.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-20	The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	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	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-21	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Functional	intersects with	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-22	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Functional	intersects with	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-39	The information system maintains a separate execution domain for each executing process.	Functional	intersects with	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SC-7(3)	The organization limits the number of external network connections to the information system.	Functional	intersects with	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
NFO - SC-7(4)	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.	Functional	intersects with	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SI-1	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].	Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SI-16	The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.	Functional	intersects with	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	5	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.
NFO - SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Functional	subset of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	10	Non-Federal Organization (NFO) controls can be found in Appendix E of NIST SP 800-171 R2. NFO controls are sourced directly from NIST SP 800-53 R4.