**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**
**Reference Document :** Secure Controls Framework (SCF) version 2025.3
**STRM Guidance:** https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

**Focal Document:** NIST SP 800-207, Zero Trust Architecture
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/207/final
**Published STRM URL:** https://securecontrolsframework.com/content/strm/scf-strm-general-nist-800-207.pdf

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | |
|---|---|---|---|---|---|---|---|---|---|
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | 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 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Asset-Service Dependencies | AST-01.1 | Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | 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 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Data Action Mapping | AST-02.8 | Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Configuration Management Database (CMDB) | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Network Diagrams & Data Flow Diagrams (DFDs) | AST-04 | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive/regulated data flows. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Asset Scope Classification | AST-04.1 | Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties). | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | 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. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Hosted Assets, Applications & Services | CLD-13 | Mechanisms exist to specify applicable cybersecurity and data protection controls that must be implemented on external Technology Assets, Applications and/or Services (TAAS), consistent with the contractual obligations established with the External Service Providers (ESP) owning, operating and/or maintaining external TAAS. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Data & Asset Classification | DCH-02 | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Sensitive Data Inventories | DCH-06.2 | Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Non-Organizationally Owned Systems / Components / Devices | DCH-13.4 | Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Information Location | DCH-24 | Mechanisms exist to identify and document the location of information and the specific system components on which the information resides. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Centralized Management Of Mobile Devices | MDM-01 | Mechanisms exist to implement and govern Mobile Device Management (MDM) controls. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Access Control For Mobile Devices | MDM-02 | Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Personally-Owned Mobile Devices | MDM-06 | Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks. | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | 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 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Inventory of Personal Data (PD) | PRI-05.5 | Mechanisms exist to establish and maintain a current inventory of all systems, applications and services that collect, receive, process, store, transmit, update and/or share Personal Data (PD). | 5 | |
| NIST Tenet 1 | N/A | All data sources and computing services are considered resources. | Functional | intersects | Third-Party Inventories | TPM-01.1 | Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Use of Cryptographic Controls | CRY-01 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Transmission Integrity | CRY-04 | Cryptographic mechanisms exist to protect the integrity of data being transmitted. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Wireless Access Authentication & Encryption | CRY-07 | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | 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 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Authenticate, Authorize and Audit (AAA) | IAC-01.2 | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP). | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | 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 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | 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 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | 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). | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Work From Anywhere (WFA) - Telecommuting Security | NET-14.5 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers. | 5 | |
| NIST Tenet 2 | N/A | All communication is secured regardless of network location. | Functional | intersects | Wireless Networking | NET-15 | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Defining Access Authorizations for Sensitive/Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Protecting Sensitive Data on External Systems | DCH-13.3 | Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Transfer Authorizations | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Authenticate, Authorize and Audit (AAA) | IAC-01.2 | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP). | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | 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 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | |
|---|---|---|---|---|---|---|---|---|---|
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Identification & Authentication for Non-Organizational Users | IAC-03 | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | 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 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Identification & Authentication for Third-Party Assets, Applications & Services | IAC-05 | Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS). | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Automated System Account Management (Directory Services) | IAC-15.1 | Automated mechanisms exist to support the management of system accounts (e.g., directory services). | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Access To Sensitive / Regulated Data | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | 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 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | 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. | 5 | |
| NIST Tenet 3 | N/A | Access to individual enterprise resources is granted on a per-session basis. | Functional | intersects | Zero Trust Architecture (ZTA) | NET-01.1 | Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Sensitive / Regulated Data Access Enforcement | CFG-08 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Sensitive / Regulated Data Protection | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is stored. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Defining Access Authorizations for Sensitive/Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Protecting Sensitive Data on External Systems | DCH-13.3 | Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Transfer Authorizations | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Automated Tools to Support Information Location | DCH-24.1 | Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity and data protection controls are in place to protect organizational information and individual data privacy. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Transfer of Sensitive and/or Regulated Data | DCH-25 | Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Transfer Activity Limits | DCH-25.1 | Mechanisms exist to establish organization-defined "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) fraudulent actions. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Enterprise Device Management (EDM) | END-01 | Mechanisms exist to facilitate the implementation of Enterprise Device Management (EDM) controls. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Authenticate, Authorize and Audit (AAA) | IAC-01.2 | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP). | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Identification & Authentication for Non-Organizational Users | IAC-03 | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | 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 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Identification & Authentication for Third-Party Assets, Applications & Services | IAC-05 | Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS). | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Privileged Access by Non-Organizational Users | IAC-05.2 | Mechanisms exist to prohibit privileged access by non-organizational users. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Identifier Management (User Names) | IAC-09 | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS). | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Federated Credential Management | IAC-13.2 | Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Automated System Account Management (Directory Services) | IAC-15.1 | Automated mechanisms exist to support the management of system accounts (e.g., directory services). | 5 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | |
|---|---|---|---|---|---|---|---|---|---|
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Mobile Device Geofencing | MDM-09 | Mechanisms exist to restrict the functionality of mobile devices based on geographic location. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Integration of Scanning & Other Monitoring Information | MON-02.3 | Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Correlation with Physical Monitoring | MON-02.4 | Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Anomalous Behavior | MON-16 | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Cross Domain Solution (CDS) | NET-02.3 | Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | 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 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | 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 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Cross Domain Authentication | NET-04.12 | Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Policy Decision Point (PDP) | NET-04.7 | Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Host Containment | NET-08.3 | Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Resource Containment | NET-08.4 | Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources. | 5 | |
| NIST Tenet 4 | N/A | Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. | Functional | intersects | Endpoint Security Validation | NET-14.7 | Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational technology assets. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Asset Governance | AST-01 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Automated Unauthorized Component Detection | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Configuration Management Program | CFG-01 | Mechanisms exist to facilitate the implementation of configuration management controls. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | System Hardening Through Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Reviews & Updates | CFG-02.1 | Mechanisms exist to review and update baseline configurations:<br>(1) At least annually;<br>(2) When required due to so; or<br>(3) As part of system component installations and upgrades. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Automated Central Management & Verification | CFG-02.2 | Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Approved Configuration Deviations | CFG-02.7 | Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Respond To Unauthorized Changes | CFG-02.8 | Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Configuration Enforcement | CFG-06 | Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Integrity Assurance & Enforcement (IAE) | CFG-06.1 | Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Change Management Program | CHG-01 | Mechanisms exist to facilitate the implementation of a change management program. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Configuration Change Control | CHG-02 | Mechanisms exist to govern the technical configuration change control processes. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Prohibition Of Changes | CHG-02.1 | Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Automated Security Response | CHG-02.4 | Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s). | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Limits of Authorized Use | DCH-13.1 | Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first:<br>(1) Verifying the implementation of required security controls; or<br>(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | subset of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Automated Tools for Real-Time Analysis | MON-01.2 | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | 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 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | |
|---|---|---|---|---|---|---|---|---|---|
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | 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. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Integration of Scanning & Other Monitoring Information | MON-02.3 | Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Zero Trust Architecture (ZTA) | NET-01.1 | Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Host Containment | NET-08.3 | Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Resource Containment | NET-08.4 | Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Automated Monitoring & Control | NET-14.1 | Automated mechanisms exist to monitor and control remote access sessions. | 5 | |
| NIST Tenet 5 | N/A | The enterprise monitors and measures the integrity and security posture of all owned and associated assets. | Functional | intersects | Endpoint Security Validation | NET-14.7 | Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational technology assets. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Automated Unauthorized Component Detection | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Network Access Control (NAC) | AST-02.5 | Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Configuration Management Database (CMDB) | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | subset of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Authenticate, Authorize and Audit (AAA) | IAC-01.2 | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP). | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | |
| NIST Tenet 6 | N/A | All resource authentication and authorization are dynamic and strictly enforced before access is allowed. | Functional | intersects | Zero Trust Architecture (ZTA) | NET-01.1 | Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Dynamic Host Configuration Protocol (DHCP) Server Logging | AST-02.6 | Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Data Action Mapping | AST-02.8 | Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Configuration Management Database (CMDB) | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Automated Tools to Support Information Location | DCH-24.1 | Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity and data protection controls are in place to protect organizational information and individual data privacy. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | subset of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Automated Tools for Real-Time Analysis | MON-01.2 | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | 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. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | 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 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | 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. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Integration of Scanning & Other Monitoring Information | MON-02.3 | Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | Endpoint Security Validation | NET-14.7 | Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational technology assets. | 5 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | 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 | |
| NIST Tenet 7 | N/A | The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. | Functional | intersects | 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 | |