## NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

**Reference document:** Secure Controls Framework (SCF) version 2026.1
**STRM Guidance:** https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

**Focal Document:** US Department of War - Cybersecurity Maturity Model Certification v2.0 - Level 2
**Focal Document URL:** https://dowcio.war.gov/CMMC/Resources-Documentation/
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-cmmc-2-level-2.pdf

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|---|---|---|---|---|---|---|---|---|---|
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other 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 | |
| ACL2-.3.1.1 | N/A | 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 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 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | 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 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | Equal | Access Enforcement | IAC-20 | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege." | 10 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | Intersects With | Third-Party Management | TPM-01 | Mechanisms exist to facilitate the implementation of third-party management controls. | 8 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | Intersects With | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| ACL2-.3.1.1 | N/A | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | Functional | Intersects With | Contract Flow-Down Requirements | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers. | 5 | |
| ACL2-.3.1.2 | N/A | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | Functional | Intersects With | 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 | |
| ACL2-.3.1.2 | N/A | 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 | |
| ACL2-.3.1.3 | N/A | 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 | |
| ACL2-.3.1.3 | N/A | Control the flow of CUI in accordance with approved authorizations. | Functional | Intersects With | 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 | |
| ACL2-.3.1.3 | N/A | Control the flow of CUI in accordance with approved authorizations. | Functional | Intersects With | Data Flow Enforcement – Access Control Lists (ACLs) | NET-04 | Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized. | 5 | |
| ACL2-.3.1.3 | N/A | Control the flow of CUI in accordance with approved authorizations. | Functional | 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 | |
| ACL2-.3.1.4 | N/A | 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 | |
| ACL2-.3.1.5 | N/A | 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 Technology Assets, Applications and/or Services (TAAS). | 5 | |
| ACL2-.3.1.5 | N/A | Employ the principle of least privilege, including for specific security functions and privileged accounts. | Functional | 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 | |
| ACL2-.3.1.5 | N/A | Employ the principle of least privilege, including for specific security functions and privileged accounts. | Functional | 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 | |
| ACL2-.3.1.5 | N/A | Employ the principle of least privilege, including for specific security functions and privileged accounts. | Functional | Intersects With | Authorize Access to Security Functions | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users. | 5 | |
| ACL2-.3.1.5 | N/A | Employ the principle of least privilege, including for specific security functions and privileged accounts. | Functional | Intersects With | Management Approval For Privileged Accounts | IAC-21.3 | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles. | 5 | |
| ACL2-.3.1.6 | N/A | 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 | |
| ACL2-.3.1.7 | N/A | 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 | |
| ACL2-.3.1.7 | N/A | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | Functional | 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 | |
| ACL2-.3.1.8 | N/A | 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 | |
| ACL2-.3.1.9 | N/A | 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 Technology Assets, Applications and/or Services (TAAS). | 10 | |
| ACL2-.3.1.9 | N/A | Provide privacy and security notices consistent with applicable CUI rules. | Functional | 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. | 5 | |
| ACL2-.3.1.9 | N/A | Provide privacy and security notices consistent with applicable CUI rules. | Functional | 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 directory services technology (e.g., Active Directory, Entra ID, etc.). | 5 | |
| ACL2-.3.1.10 | N/A | 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 | |
| ACL2-.3.1.10 | N/A | Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. | Functional | 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 | |
| ACL2-.3.1.11 | N/A | 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 | |
| ACL2-.3.1.12 | N/A | 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 | |
| ACL2-.3.1.12 | N/A | 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 | |
| ACL2-.3.1.12 | N/A | Monitor and control remote access sessions. | Functional | Intersects With | 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 | |
| ACL2-.3.1.13 | N/A | 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 | |
| ACL2-.3.1.14 | N/A | 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 | |
| ACL2-.3.1.15 | N/A | 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 | |
| ACL2-.3.1.16 | N/A | 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 | |
| ACL2-.3.1.17 | N/A | Protect wireless access using authentication and encryption. | Functional | Intersects With | Authentication & Encryption | NET-15.1 | Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by:(1) Authenticating devices trying to connect; and(2) Encrypting transmitted data. | 5 | |
| ACL2-.3.1.18 | N/A | 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 | |
| ACL2-.3.1.18 | N/A | Control connection of mobile devices. | Functional | Equal | Access Control For Mobile Devices | MDM-02 | Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS). | 10 | |
| ACL2-.3.1.18 | N/A | Control connection of mobile devices. | Functional | Intersects With | Personally-Owned Mobile Devices | MDM-06 | Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS). | 5 | |
| ACL2-.3.1.18 | N/A | Control connection of mobile devices. | Functional | 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 | |
| ACL2-.3.1.19 | N/A | 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 | |
| ACL2-.3.1.20 | N/A | Verify and control/limit connections to and use of external systems. | Functional | Equal | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13 | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data. | 10 | |
| ACL2-.3.1.20 | N/A | 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, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first:(1) Verifying the implementation of required security, compliance and/or resilience controls; or(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5 | |
| ACL2-.3.1.20 | N/A | Verify and control/limit connections to and use of external systems. | Functional | Intersects With | Ad-Hoc Transfers | DCH-17 | Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties. | 3 | |
| ACL2-.3.1.21 | N/A | 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 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | 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. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | 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. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Multi-Tenant Environments | 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 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Sensitive Data In Public Cloud Providers | CLD-10 | Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers. | 5 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Publicly Accessible Content | DCH-15 | Mechanisms exist to control publicly-accessible content. | 5 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Terms of Employment | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | 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. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | 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. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Web Security | WEB-01 | Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures. | 5 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Use of Demilitarized Zones (DMZ) | WEB-02 | Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports. | 3 | |
| ACL2-.3.1.22 | N/A | Control CUI posted or processed on publicly accessible systems. | Functional | Intersects With | Client-Facing Web Services | WEB-04 | Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service. | 5 | |
| ATL2-.3.2.1 | N/A | 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 | Intersects With | Formal Indoctrination | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access. | 8 | |
| ATL2-.3.2.1 | N/A | 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 | Security, Compliance & Resilience Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function. | 10 | |
| ATL2-.3.2.2 | N/A | Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. | Functional | Intersects With | Formal Indoctrination | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access. | 8 | |

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|---|---|---|---|---|---|---|---|---|---|
| ATL2.-3.2.2 | N/A | Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. | Functional | Equal | Role-Based Security, Compliance & Resilience Training | SAT-03 | Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter. | 10 | |
| ATL2.-3.2.3 | N/A | Provide security awareness training on recognizing and reporting potential indicators of insider threat. | Functional | Intersects With | Cyber Threat Environment | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations. | 8 | |
| ATL2.-3.2.3 | N/A | 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 | |
| AUL2.-3.3.1 | N/A | 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 | |
| AUL2.-3.3.1 | N/A | 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 | 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 | |
| AUL2.-3.3.2 | N/A | 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 Technology Assets, Applications and/or Services (TAAS) 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 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | Functional | Intersects With | Secure 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. | 8 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | 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. | 8 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | Functional | Intersects With | Baseline Tailoring | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success. | 8 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | Functional | Subset Of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | Functional | Intersects With | Security Event Monitoring | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures. | 8 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | Functional | Intersects With | Analyze and Prioritize Monitoring Requirements | MON-01.16 | Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes. | 8 | |
| AUL2.-3.3.3 | N/A | Review and update logged events. | 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 | |
| AUL2.-3.3.4 | N/A | 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 | |
| AUL2.-3.3.5 | N/A | 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 | |
| AUL2.-3.3.5 | N/A | Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. | 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 | |
| AUL2.-3.3.6 | N/A | 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 | |
| AUL2.-3.3.6 | N/A | Provide audit record reduction and report generation to support on-demand analysis and reporting. | Functional | 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 | |
| AUL2.-3.3.7 | N/A | 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 | |
| AUL2.-3.3.7 | N/A | Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | Functional | Intersects With | Clock Synchronization | SEA-20 | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks. | 5 | |
| AUL2.-3.3.8 | N/A | 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 | |
| AUL2.-3.3.8 | N/A | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | Functional | Intersects With | Sensitive Event Log Information | MON-03.1 | Mechanisms exist to protect sensitive/regulated data contained in log files. | 5 | |
| AUL2.-3.3.8 | N/A | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | Functional | Equal | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | |
| AUL2.-3.3.9 | N/A | 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 | |
| AUL2.-3.3.9 | N/A | Limit management of audit logging functionality to a subset of privileged users. | Functional | 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 | |
| CML2.-3.4.1 | N/A | 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 | |
| CML2.-3.4.1 | N/A | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | Functional | Intersects With | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel. | 5 | |
| CML2.-3.4.1 | N/A | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | Functional | Intersects With | Secure 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 | |
| CML2.-3.4.2 | N/A | Establish and enforce security configuration settings for information technology products employed in organizational systems. | Functional | Equal | Secure 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. | 10 | |
| CML2.-3.4.3 | N/A | 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 | |
| CML2.-3.4.3 | N/A | Track, review, approve or disapprove, and log changes to organizational systems. | Functional | Equal | Configuration Change Control | CHG-02 | Mechanisms exist to govern the technical configuration change control processes. | 10 | |
| CML2.-3.4.4 | N/A | 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 | |
| CML2.-3.4.5 | N/A | 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 | |
| CML2.-3.4.5 | N/A | Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. | Functional | 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 Technology Assets, Applications and/or Services (TAAS). | 5 | |
| CML2.-3.4.6 | N/A | 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 | |
| CML2.-3.4.7 | N/A | 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 | |
| CML2.-3.4.7 | N/A | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | Functional | Intersects With | Prevent Unauthorized Software Execution | CFG-03.2 | Mechanisms exist to configure systems to prevent the execution of unauthorized software programs. | 5 | |
| CML2.-3.4.8 | N/A | 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 | |
| CML2.-3.4.9 | N/A | 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 | |
| CML2.-3.4.9 | N/A | Control and monitor user-installed software. | Functional | Intersects With | Prohibit Installation Without Privileged Status | END-03 | Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status. | 5 | |
| IAL2.-3.5.1 | N/A | 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 | |
| IAL2.-3.5.1 | N/A | Identify system users, processes acting on behalf of users, and devices. | Functional | 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 | |
| IAL2.-3.5.1 | N/A | Identify system users, processes acting on behalf of users, and devices. | Functional | 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). | 8 | |
| IAL2.-3.5.2 | N/A | 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 | |
| IAL2.-3.5.2 | N/A | 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 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 | |
| IAL2.-3.5.2 | N/A | Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. | Functional | 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 | |
| IAL2.-3.5.3 | N/A | 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 Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data. | 5 | |
| IAL2.-3.5.3 | N/A | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | Functional | 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 | |
| IAL2.-3.5.3 | N/A | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | Functional | 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 | |
| IAL2.-3.5.3 | N/A | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | Functional | 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 | |
| IAL2.-3.5.4 | N/A | 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 | |
| IAL2.-3.5.5 | N/A | 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 Technology Assets, Applications and/or Services (TAAS). | 10 | |
| IAL2.-3.5.6 | N/A | 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 | |
| IAL2.-3.5.7 | N/A | 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 | |
| IAL2.-3.5.8 | N/A | Prohibit password reuse for a specified number of generations. | Functional | Subset Of | Authenticator Management | IAC-10 | Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 10 | |
| IAL2.-3.5.9 | N/A | Allow temporary password use for system logons with an immediate change to a permanent password. | Functional | Subset Of | Authenticator Management | IAC-10 | Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 10 | |

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|---|---|---|---|---|---|---|---|---|---|
| IAL2.-3.5.10 | N/A | 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 | |
| IAL2.-3.5.11 | N/A | 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 | |
| IRL2.-3.6.1 | N/A | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | Functional | Subset Of | 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 | |
| IRL2.-3.6.1 | N/A | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | Functional | Intersects With | Incident Response Training | IRO-05 | Mechanisms exist to train personnel in their incident response roles and responsibilities. | 5 | |
| IRL2.-3.6.2 | N/A | Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. | Functional | Subset Of | 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 | |
| IRL2.-3.6.3 | N/A | 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 | |
| MAL2.-3.7.1 | N/A | Perform maintenance on organizational systems. | Functional | Subset Of | Controlled Maintenance | MNT-02 | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS). | 10 | |
| MAL2.-3.7.2 | N/A | Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. | Functional | Subset Of | Maintenance Tools | MNT-04 | Mechanisms exist to control and monitor the use of system maintenance tools. | 10 | |
| MAL2.-3.7.3 | N/A | Ensure equipment removed for off-site maintenance is sanitized of any CUI. | Functional | Subset Of | 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 | |
| MAL2.-3.7.4 | N/A | 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 | |
| MAL2.-3.7.5 | N/A | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | 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 Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data. | 8 | |
| MAL2.-3.7.5 | N/A | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | Functional | Subset Of | Remote Maintenance | MNT-05 | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities. | 10 | |
| MAL2.-3.7.5 | N/A | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | Functional | Intersects With | Remote Maintenance Disconnect Verification | MNT-05.4 | Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated. | 3 | |
| MAL2.-3.7.6 | N/A | Supervise the maintenance activities of maintenance personnel without required access authorization. | Functional | Intersects With | Authorized Maintenance Personnel | MNT-06 | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel. | 5 | |
| MAL2.-3.7.6 | N/A | Supervise the maintenance activities of maintenance personnel without required access authorization. | Functional | Intersects With | Maintenance Personnel Without Appropriate Access | MNT-06.1 | Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated. | 5 | |
| MAL2.-3.7.6 | N/A | Supervise the maintenance activities of maintenance personnel without required access authorization. | Functional | Intersects With | Non-System Related Maintenance | MNT-06.2 | Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations. | 5 | |
| MPL2.-3.8.1 | N/A | 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 | |
| MPL2.-3.8.1 | N/A | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | Functional | 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 | |
| MPL2.-3.8.2 | N/A | 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 | |
| MPL2.-3.8.3 | N/A | Sanitize or destroy system media containing CUI before disposal or release for reuse. | 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 | |
| MPL2.-3.8.3 | N/A | Sanitize or destroy system media containing CUI before disposal or release for reuse. | Functional | Intersects With | Secure Disposal, Destruction or Re-Use of Equipment | AST-09 | Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components. | 8 | |
| MPL2.-3.8.3 | N/A | Sanitize or destroy system media containing CUI before disposal or release for reuse. | Functional | Intersects With | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 3 | |
| MPL2.-3.8.3 | N/A | Sanitize or destroy system media containing CUI before disposal or release for reuse. | Functional | Equal | Physical Media Disposal | DCH-08 | Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures. | 10 | |
| MPL2.-3.8.3 | N/A | Sanitize or destroy system media containing CUI before disposal or release for reuse. | Functional | Intersects With | 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. | 8 | |
| MPL2.-3.8.4 | N/A | 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 | |
| MPL2.-3.8.5 | N/A | 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 | |
| MPL2.-3.8.6 | N/A | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | Functional | Intersects With | Alternate Physical Protection | CRY-01.1 | Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards. | 5 | |
| MPL2.-3.8.6 | N/A | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | Functional | Intersects With | Encrypting Data At Rest | CRY-05 | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest. | 8 | |
| MPL2.-3.8.7 | N/A | 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 | |
| MPL2.-3.8.8 | N/A | 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 systems when such devices have no identifiable owner. | 10 | |
| MPL2.-3.8.9 | N/A | 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 5 | |
| MPL2.-3.8.9 | N/A | Protect the confidentiality of backup CUI at storage locations. | Functional | Intersects With | Cryptographic Protection | BCD-11.4 | Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information. | 5 | |
| PSL2.-3.9.1 | N/A | Screen individuals prior to authorizing access to organizational systems containing CUI. | Functional | Subset Of | Personnel Screening | HRS-04 | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access. | 10 | |
| PSL2.-3.9.1 | N/A | Screen individuals prior to authorizing access to organizational systems containing CUI. | Functional | Intersects With | Roles With Special Protection Measures | HRS-04.1 | Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria. | 5 | |
| PSL2.-3.9.2 | N/A | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | Functional | Intersects With | Onboarding, Transferring & Offboarding Personnel | HRS-01.1 | Mechanisms exist to proactively govern the following personnel management actions:(1) Onboarding new personnel (e.g., new hires);(2) Transferring personnel into new roles within the organization; and(3) Offboarding personnel (e.g., termination of employment). | 8 | |
| PSL2.-3.9.2 | N/A | 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 Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner. | 8 | |
| PSL2.-3.9.2 | N/A | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | Functional | Intersects With | Personnel Termination | HRS-09 | Mechanisms exist to govern the termination of individual employment. | 8 | |
| PEL2.-3.10.1 | N/A | 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 | |
| PEL2.-3.10.1 | N/A | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | Functional | Intersects With | Role-Based Physical Access | PES-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual. | 5 | |
| PEL2.-3.10.1 | N/A | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | Functional | Intersects With | Access To Critical Systems | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility. | 5 | |
| PEL2.-3.10.1 | N/A | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | Functional | 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 | |
| PEL2.-3.10.1 | N/A | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | Functional | 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 | |
| PEL2.-3.10.1 | N/A | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | Functional | 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 | |
| PEL2.-3.10.2 | N/A | 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 | |
| PEL2.-3.10.2 | N/A | Protect and monitor the physical facility and support infrastructure for organizational systems. | Functional | Intersects With | Monitoring Physical Access | PES-05 | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents. | 5 | |
| PEL2.-3.10.2 | N/A | Protect and monitor the physical facility and support infrastructure for organizational systems. | Functional | Intersects With | Intrusion Alarms / Surveillance Equipment | PES-05.1 | Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment. | 5 | |
| PEL2.-3.10.2 | N/A | Protect and monitor the physical facility and support infrastructure for organizational systems. | Functional | Intersects With | Monitoring Physical Access To Critical Systems | PES-05.2 | Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility. | 5 | |
| PEL2.-3.10.3 | N/A | Escort visitors and monitor visitor activity. | Functional | Subset Of | 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 | |
| PEL2.-3.10.3 | N/A | 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 | |
| PEL2.-3.10.3 | N/A | Escort visitors and monitor visitor activity. | Functional | Intersects With | Distinguish Visitors from On-Site Personnel | PES-06.1 | Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible. | 5 | |
| PEL2.-3.10.3 | N/A | Escort visitors and monitor visitor activity. | Functional | 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 | |
| PEL2.-3.10.4 | N/A | 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 | |
| PEL2.-3.10.5 | N/A | 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 | |
| PEL2.-3.10.5 | N/A | Control and manage physical access devices. | Functional | 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 | |
| PEL2.-3.10.6 | N/A | Enforce safeguarding measures for CUI at alternate work sites. | Functional | Intersects With | Sensitive / Regulated Data Protection | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored. | 8 | |
| PEL2.-3.10.6 | N/A | 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 Technology Assets, Applications, Services and/or Data (TAASD) for remote workers. | 5 | |
| PEL2.-3.10.6 | N/A | Enforce safeguarding measures for CUI at alternate work sites. | Functional | Subset Of | Alternate Work Site | PES-11 | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites. | 10 | |
| RAL2.-3.11.1 | N/A | 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 Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|---|---|---|---|---|---|---|---|---|---|
| RAL2-.3.11.2 | N/A | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | Functional | Subset Of | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 10 | |
| RAL2-.3.11.2 | N/A | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | Functional | Intersects With | Privileged Access | VPM-06.3 | Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities. | 5 | |
| RAL2-.3.11.3 | N/A | Remediate vulnerabilities in accordance with risk assessments. | Functional | Intersects With | Risk Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. | 8 | |
| RAL2-.3.11.3 | N/A | Remediate vulnerabilities in accordance with risk assessments. | Functional | Intersects With | Continuous Vulnerability Remediation Activities | VPM-04 | Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks. | 8 | |
| RAL2-.3.11.3 | N/A | Remediate vulnerabilities in accordance with risk assessments. | Functional | Intersects With | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 8 | |
| CAL2-.3.12.1 | N/A | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | Functional | Equal | Security, Compliance & Resilience Controls Oversight | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership. | 10 | |
| CAL2-.3.12.1 | N/A | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | Functional | 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 | |
| CAL2-.3.12.1 | N/A | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | Functional | Intersects With | Security, Compliance & Resilience Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements. | 5 | |
| CAL2-.3.12.1 | N/A | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | Functional | Intersects With | Assessments | IAO-02 | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements. | 5 | |
| CAL2-.3.12.2 | N/A | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. | Functional | Equal | Capabilities Deficiency Tracking | IAO-05 | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification;(6) Status of planned corrective actions, if applicable;(7) | 10 | |
| CAL2-.3.12.3 | N/A | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | Functional | Subset Of | Security, Compliance & Resilience Controls Oversight | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership. | 10 | |
| CAL2-.3.12.3 | N/A | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | Functional | Intersects With | Threat Intelligence 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. | 3 | |
| CAL2-.3.12.3 | N/A | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | Functional | Intersects With | Threat Intelligence 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 | |
| CAL2-.3.12.4 | N/A | 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 | Subset Of | Applied Security, Compliance and Resilience Controls Documentation | IAO-03 | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including | 10 | |
| CAL2-.3.12.4 | N/A | 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 | 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 | |
| SCL2-.3.13.1 | N/A | 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 | Network Security Controls (NSC) | NET-01 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 10 | |
| SCL2-.3.13.1 | N/A | 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 | Intersects With | Guest Networks | NET-02.2 | Mechanisms exist to implement and manage a secure guest network. | 10 | |
| SCL2-.3.13.1 | N/A | 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 | |
| SCL2-.3.13.2 | N/A | 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 | |
| SCL2-.3.13.2 | N/A | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | Functional | Subset Of | Secure Engineering Principles | SEA-01 | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 10 | |
| SCL2-.3.13.2 | N/A | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | Functional | Intersects With | Defense-In-Depth (DiD) Architecture | SEA-03 | Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. | 3 | |
| SCL2-.3.13.3 | N/A | 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 | |
| SCL2-.3.13.4 | N/A | 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 | |
| SCL2-.3.13.5 | N/A | 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 Technology Assets, Applications and/or Services (TAAS) to protect from other network resources. | 5 | |
| SCL2-.3.13.6 | N/A | 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 | |
| SCL2-.3.13.7 | N/A | 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 | |
| SCL2-.3.13.8 | N/A | 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 | |
| SCL2-.3.13.8 | N/A | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| SCL2-.3.13.9 | N/A | 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 | |
| SCL2-.3.13.10 | N/A | 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 | |
| SCL2-.3.13.10 | N/A | Establish and manage cryptographic keys for cryptography employed in organizational systems. | Functional | 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 | |
| SCL2-.3.13.11 | N/A | 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 | |
| SCL2-.3.13.12 | N/A | 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 | |
| SCL2-.3.13.13 | N/A | 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 | |
| SCL2-.3.13.14 | N/A | 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 | |
| SCL2-.3.13.15 | N/A | Protect the authenticity of communications sessions. | Functional | Equal | Session Integrity | NET-09 | Mechanisms exist to protect the authenticity and integrity of communications sessions. | 10 | |
| SCL2-.3.13.16 | N/A | Protect the confidentiality of CUI at rest. | Functional | Intersects With | Encrypting Data At Rest | CRY-05 | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest. | 8 | |
| SCL2-.3.13.16 | N/A | Protect the confidentiality of CUI at rest. | Functional | Intersects With | Endpoint Protection Measures | END-02 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 8 | |
| SIL2-.3.14.1 | N/A | 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 | |
| SIL2-.3.14.1 | N/A | Identify, report, and correct system flaws in a timely manner. | Functional | Intersects With | Vulnerability Remediation Process | VPM-02 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 8 | |
| SIL2-.3.14.1 | N/A | Identify, report, and correct system flaws in a timely manner. | Functional | Intersects With | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 8 | |
| SIL2-.3.14.2 | N/A | Provide protection from malicious code at designated locations within organizational systems. | Functional | Subset Of | Endpoint Device Management (EDM) | END-01 | Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls. | 10 | |
| SIL2-.3.14.2 | N/A | 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 | |
| SIL2-.3.14.3 | N/A | Monitor system security alerts and advisories and take action in response. | Functional | Equal | Security Event Monitoring | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures. | 10 | |
| SIL2-.3.14.3 | N/A | Monitor system security alerts and advisories and take action in response. | Functional | Subset Of | Threat Intelligence 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 | |
| SIL2-.3.14.3 | N/A | Monitor system security alerts and advisories and take action in response. | Functional | Intersects With | Threat Intelligence 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 | |
| SIL2-.3.14.4 | N/A | Update malicious code protection mechanisms when new releases are available. | Functional | Equal | Automatic Antimalware Signature Updates | END-04.1 | Automated mechanisms exist to update antimalware technologies, including signature definitions. | 10 | |
| SIL2-.3.14.5 | N/A | 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 | |
| SIL2-.3.14.6 | N/A | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Functional | Subset Of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| SIL2-.3.14.6 | N/A | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Functional | Intersects With | Inbound & Outbound Communications Traffic | MON-01.3 | Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. | 8 | |
| SIL2-.3.14.6 | N/A | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Functional | 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. | 8 | |
| SIL2-.3.14.7 | N/A | Identify unauthorized use of organizational systems. | Functional | Intersects With | 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. | 8 | |
| SIL2-.3.14.7 | N/A | Identify unauthorized use of organizational systems. | Functional | Intersects With | Monitoring for Indicators of Compromise (IOC) | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC). | 8 | |
| SIL2-.3.14.7 | N/A | Identify unauthorized use of organizational systems. | Functional | Intersects With | 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. | 8 | |
| SIL2-.3.14.7 | N/A | Identify unauthorized use of organizational systems. | Functional | Intersects With | Indicators of Compromise (IOC) | IRO-03 | Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events. | 8 | |