**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**
**Reference docume** Secure Controls Framework (SCF) version 2026.1
**STRM Guidance:** https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

**Focal Document:** **NIST SP 800-53 Rev 5.2 Security and Privacy Controls for Information Systems and Organiz**
**Focal Document U** https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
**Published STRM U** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-53-r5-2-mod.pdf

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| AC-02(01) | Management \| Automated System Account | Support the management of system accounts using [Assignment: organization-defined automated mechanisms]. | 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 | |
| AC-02(02) | Account Management \| Automated Temporary and Emergency Account Management | Automatically [Selection (one): remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. | Functional | Equal | Removal of Temporary / Emergency Accounts | IAC-15.2 | Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account. | 10 | |
| AC-02(03) | Account Management \| Disable Accounts | Disable accounts within [Assignment: organization-defined time period] when the accounts:a. Have expired;b. Are no longer associated with a user or individual;c. Are in violation of organizational policy; ord. Have been inactive for [Assignment: organization-defined time period]. | Functional | Equal | Disable Inactive Accounts | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period. | 10 | |
| AC-02(04) | Account Management \| Automated Audit Actions | Automatically audit account creation, modification, enabling, disabling, and removal actions. | Functional | Equal | Automated Audit Actions | IAC-15.4 | Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles. | 10 | |
| AC-02(05) | Account Management \| Inactivity Logout | Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out]. | 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 | |
| AC-02(13) | Account Management \| Disable Accounts for High-risk Individuals | Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks]. | Functional | Intersects With | High-Risk Terminations | HRS-09.2 | Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management. | 5 | |
| AC-02(13) | Account Management \| Disable Accounts for High-risk Individuals | Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks]. | Functional | Intersects With | Account Disabling for High Risk Individuals | IAC-15.6 | Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization. | 5 | |
| AC-04 | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies]. | Functional | Equal | 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. | 10 | |
| AC-05 | Separation of Duties | a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties. | Functional | Intersects With | Input Data Validation | TDA-18 | Mechanisms exist to check the validity of information inputs. | 5 | |
| AC-05 | Separation of Duties | a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties. | Functional | Intersects With | Dual Authorization for Change | CHG-04.3 | Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS). | 5 | |
| AC-05 | Separation of Duties | a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties. | Functional | Intersects With | Safeguarding Data Over Open Networks | NET-12 | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks. | 5 | |
| AC-05 | Separation of Duties | a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties. | Functional | Intersects With | Separation of Duties (SoD) | HRS-11 | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion. | 5 | |
| AC-06 | Least Privilege | Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | 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 | |
| AC-06 | Least Privilege | Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | Functional | Intersects With | Access Enforcement | IAC-20 | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege." | 5 | |
| AC-06(01) | Least Privilege \| Authorize Access to Security Functions | Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; andb. [Assignment: organization-defined security-relevant information]. | Functional | Equal | Authorize Access to Security Functions | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users. | 10 | |
| AC-06(02) | Least Privilege \| Non-privileged Access for Nonsecurity Functions | Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] 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 | |
| AC-06(05) | Least Privilege \| Privileged Accounts | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. | Functional | Equal | Management Approval For Privileged Accounts | IAC-21.3 | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles. | 10 | |
| AC-06(07) | Least Privilege \| Review of User Privileges | a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; andb. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs. | Functional | Equal | Periodic Review of Account Privileges | IAC-17 | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary. | 10 | |
| AC-06(09) | Least Privilege \| Log Use of Privileged Functions | Log the execution of privileged functions. | Functional | Equal | Auditing Use of Privileged Functions | IAC-21.4 | Mechanisms exist to audit the execution of privileged functions. | 10 | |
| AC-06(10) | Least Privilege \| Prohibit Non-privileged Users from Executing Privileged Functions | Prevent non-privileged users from executing privileged functions. | 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 | |
| AC-11 | Device Lock | a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; andb. Retain the device lock until the user reestablishes access using established identification and authentication procedures. | Functional | Intersects With | 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. | 5 | |
| AC-11(01) | Device Lock \| Pattern-hiding Displays | Conceal, via the device lock, information previously visible on the display with a publicly viewable image. | Functional | Equal | 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. | 10 | |
| AC-12 | Session Termination | Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect]. | 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 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| AC-17(01) | Remote Access \| Monitoring and Control | Employ automated mechanisms to monitor and control remote access methods. | Functional | Equal | Automated Monitoring & Control | NET-14.1 | Automated mechanisms exist to monitor and control remote access sessions. | 10 | |
| AC-17(02) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | Implement cryptographic mechanisms to protect the confidentiality and integrity 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 | |
| AC-17(03) | Remote Access \| Managed Access Control Points | Route remote accesses through authorized and managed network 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 | |
| AC-17(04) | Remote Access \| Privileged Commands and Access | a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; andb. Document the rationale for remote access in the security plan for the system. | 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 | |
| AC-18(01) | Wireless Access \| Authentication and Encryption | Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. | Functional | Equal | 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 | 10 | |
| AC-18(03) | Wireless Access \| Disable Wireless Networking | Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment. | Functional | Equal | Disable Wireless Networking | NET-15.2 | Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users. | 10 | |
| AC-19(05) | Access Control for Mobile Devices \| Full Device or Container-based Encryption | Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. | 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 | |
| AC-20(01) | Use of External Systems \| Limits on Authorized Use | Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; orb. Retention of approved system connection or processing agreements with the organizational entity hosting the external system. | Functional | Equal | 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 | 10 | |
| AC-20(02) | Use of External Systems \| Portable Storage Devices — Restricted Use | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions]. | Functional | Intersects With | Portable Storage Devices | DCH-13.2 | Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems. | 5 | |
| AC-21 | Information Sharing | a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; andb. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions. | Functional | Intersects With | Information Sharing With Third Parties | PRI-07 | Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject. | 5 | |
| AC-21 | Information Sharing | a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; andb. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions. | Functional | Intersects With | Information Sharing | DCH-14 | Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected. | 5 | |
| AT-02(03) | Literacy Training and Awareness \| Social Engineering and Mining | Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. | Functional | Equal | Social Engineering & Mining | SAT-02.2 | Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social | 10 | |
| AU-03(01) | Content of Audit Records \| Additional Audit Information | Generate audit records containing the following additional information: [Assignment: organization-defined additional information]. | Functional | Intersects With | Sensitive Event Log Information | MON-03.1 | Mechanisms exist to protect sensitive/regulated data contained in log files. | 5 | |
| AU-06(01) | Audit Record Review, Analysis, and Reporting \| Automated Process Integration | Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms]. | Functional | Intersects With | Sensitive Event Log Information | MON-03.1 | Mechanisms exist to protect sensitive/regulated data contained in log files. | 5 | |
| AU-06(03) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | Analyze and correlate audit records across different repositories to gain organization-wide situational awareness. | 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. | 5 | |
| AU-07 | Audit Record Reduction and Report Generation | Provide and implement an audit record reduction and report generation capability that:a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; andb. Does not alter the original content or time ordering of audit records. | 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 | |
| AU-07(01) | Audit Record Reduction and Report Generation \| Automatic Processing | Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records]. | 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 | |
| AU-09(04) | Protection of Audit Information \| Access by Subset of Privileged Users | Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles]. | 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 | |
| CA-02(01) | Control Assessments \| Independent Assessors | Employ independent assessors or assessment teams to conduct control assessments. | Functional | Equal | Assessor Independence | IAO-02.1 | Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments. | 10 | |
| CA-07(01) | Continuous Monitoring \| Independent Assessment | Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis. | Functional | Intersects With | Independent Assessors | CPL-03.1 | Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant | 5 | |
| CA-07(01) | Continuous Monitoring \| Types of Assessments | Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis. | Functional | Intersects With | Security, Compliance & Resilience Controls Oversight | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership. | 5 | |
| CM-02(02) | Baseline Configuration \| Automation Support for Accuracy and Currency | Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | 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 | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| CM-02(03) | Configuration \| Retention of Previous Configurations | Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback. | Functional | Equal | Retention Of Previous Configurations | CFG-02.3 | Mechanisms exist to retain previous versions of baseline configuration to support roll back. | 10 | |
| CM-02(07) | Baseline Configuration \| Configure Systems and Components for High-risk Areas | a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls]. | Functional | Equal | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations. | 10 | |
| CM-03 | Configuration Change Control | the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration | Functional | Subset Of | Change Management Program | CHG-01 | Mechanisms exist to facilitate the implementation of a change management program. | 10 | |
| CM-03 | Configuration Change Control | the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration | Functional | Intersects With | Configuration Change Control | CHG-02 | Mechanisms exist to govern the technical configuration change control processes. | 5 | |
| CM-03(02) | Configuration Change Control \| Testing, Validation, and Documentation of Changes | Test, validate, and document changes to the system before finalizing the implementation of the changes. | Functional | Intersects With | Control Functionality Verification | CHG-06 | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed. | 5 | |
| CM-03(02) | Configuration Change Control \| Testing, Validation, and Documentation of Changes | Test, validate, and document changes to the system before finalizing the implementation of the changes. | Functional | Intersects With | Test, Validate & Document Changes | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment. | 5 | |
| CM-03(04) | Configuration Change Control \| Security and Privacy Representatives | Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element]. | Functional | Equal | Security, Compliance & Resilience Representative for Asset Lifecycle Changes | CHG-02.3 | Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process. | 10 | |
| CM-04(02) | Impact Analyses \| Verification of Controls | After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system. | Functional | Equal | Technical Verification | IAO-06 | Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls. | 10 | |
| CM-07(01) | Least Functionality \| Periodic Review | a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; andb. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure]. | 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 | |
| CM-07(02) | Least Functionality \| Prevent Program Execution | Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. | Functional | Intersects With | Prevent Program Execution | SEA-06 | Automated mechanisms exist to prevent the execution of unauthorized software programs. | 5 | |
| CM-07(02) | Least Functionality \| Prevent Program Execution | Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. | Functional | Intersects With | Prevent Unauthorized Software Execution | CFG-03.2 | Mechanisms exist to configure systems to prevent the execution of unauthorized software programs. | 5 | |
| CM-07(05) | Least Functionality \| Authorized Software — Allow-by-exception | a. Identify [Assignment: organization-defined software programs authorized to execute on the system];b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; andc. Review and update the list of authorized software programs [Assignment: organization-defined frequency]. | 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 | |
| CM-08(01) | System Component Inventory \| Updates During Installation and Removal | Update the inventory of system components as part of component installations, removals, and system updates. | Functional | Equal | Updates During Installations / Removals | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades. | 10 | |
| CM-08(03) | System Component Inventory \| Automated Unauthorized Component Detection | a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]]. | Functional | Intersects With | 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 | |
| CM-08(03) | System Component Inventory \| Automated Unauthorized Component Detection | a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]]. | Functional | Intersects With | Software Installation Alerts | END-03.1 | Mechanisms exist to generate an alert when new software is detected. | 5 | |
| CM-08(03) | System Component Inventory \| Automated Unauthorized Component Detection | a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]]. | Functional | Intersects With | Unauthorized Installation Alerts | CFG-05.1 | Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected. | 5 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| CM-09 | Configuration Management Plan | Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification. | Functional | Subset Of | Configuration Management Program | CFG-01 | Mechanisms exist to facilitate the implementation of configuration management controls. | 10 | |
| CM-09 | Configuration Management Plan | Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification. | Functional | Intersects With | Stakeholder Notification of Changes | CHG-05 | Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes. | 5 | |
| CM-12 | Information Location | a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored;b. Identify and document the users who have access to the system and system components where the information is processed and stored; andc. Document changes to the location (i.e., system or system components) where the information is processed and stored. | Functional | Equal | Information Location | DCH-24 | Mechanisms exist to identify and document the location of information and the specific system components on which the information resides. | 10 | |
| CM-12(01) | Information Location \| Automated Tools to Support Information Location | Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy. | Functional | Equal | Automated Tools to Support Information Location | DCH-24.1 | Automated mechanisms exist to identify by data classification type to ensure adequate security, compliance and resilience controls are in place to protect organizational information and individual data protection. | 10 | |
| CP-02(01) | Contingency Plan \| Coordinate with Related Plans | Coordinate contingency plan development with organizational elements responsible for related plans. | Functional | Equal | Coordinate with Related Plans | BCD-01.1 | Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans. | 10 | |
| CP-02(03) | Contingency Plan \| Resume Mission and Business Functions | Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation. | Functional | Intersects With | Resume All Missions & Business Functions | BCD-02.1 | Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation. | 5 | |
| CP-02(03) | Contingency Plan \| Resume Mission and Business Functions | Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation. | Functional | Intersects With | Resume Essential Missions & Business Functions | BCD-02.3 | Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation. | 5 | |
| CP-02(08) | Contingency Plan \| Identify Critical Assets | Identify critical system assets supporting [Selection (one): all; essential] mission and business functions. | Functional | Equal | Identify Critical Assets | BCD-02 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 10 | |
| CP-04(01) | Contingency Plan Testing \| Coordinate with Related Plans | Coordinate contingency plan testing with organizational elements responsible for related plans. | Functional | Equal | Coordinated Testing with Related Plans | BCD-04.1 | Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans. | 10 | |
| CP-06 | Alternate Storage Site | a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; andb. Ensure that the alternate storage site provides controls equivalent to that of the primary site. | Functional | Equal | Alternate Storage Site | BCD-08 | Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information. | 10 | |
| CP-06(01) | Alternate Storage Site \| Separation from Primary Site | Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | Functional | Equal | Separation from Primary Storage Site | BCD-08.1 | Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats. | 10 | |
| CP-06(03) | Alternate Storage Site \| Accessibility | Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. | Functional | Equal | Primary Storage Site Accessibility | BCD-08.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage sites in the event of an area-wide disruption or disaster. | 10 | |
| CP-07 | Alternate Processing Site | a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; andc. Provide controls at the alternate processing site that are equivalent to those at the primary site. | Functional | Equal | Alternate Processing Site | BCD-09 | Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site. | 10 | |
| CP-07(01) | Alternate Processing Site \| Separation from Primary Site | Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats. | Functional | Equal | Separation from Primary Processing Site | BCD-09.1 | Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats. | 10 | |
| CP-07(02) | Alternate Processing Site \| Accessibility | Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. | Functional | Equal | Alternate Processing Site Accessibility | BCD-09.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing sites and possible mitigation actions, in the event of an area-wide disruption or disaster. | 10 | |
| CP-07(03) | Alternate Processing Site \| Priority of Service | Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives). | Functional | Equal | Alternate Site Priority of Service | BCD-09.3 | Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs). | 10 | |
| CP-08 | Telecommunications Services | Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. | Functional | Intersects With | Telecommunications Services Availability | BCD-10 | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services. | 5 | |
| CP-08(01) | Telecommunications Services \| Priority of Service Provisions | a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); andb. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier. | Functional | Equal | Telecommunications Priority of Service Provisions | BCD-10.1 | Mechanisms exist to formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs). | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| CP-08(02) | Telecommunications Services \| Single Points of Failure | Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services. | Functional | Intersects With | Telecommunications Services Availability | BCD-10 | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services. | 5 | |
| CP-09(01) | System Backup \| Testing for Reliability and Integrity | Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity. | Functional | Equal | Testing for Reliability & Integrity | BCD-11.1 | Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data. | 10 | |
| CP-09(08) | System Backup \| Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information]. | Functional | Equal | Cryptographic Protection | BCD-11.4 | Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information. | 10 | |
| CP-10(02) | System Recovery and Reconstitution \| Transaction Recovery | Implement transaction recovery for systems that are transaction-based. | Functional | Equal | Transaction Recovery | BCD-12.1 | Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point | 10 | |
| IA-03 | Device Identification and Authentication | Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection. | 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 | |
| IA-04(04) | Identifier Management \| Identify User Status | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status]. | Functional | Intersects With | 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 | |
| IA-04(04) | Identifier Management \| Identify User Status | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status]. | Functional | Intersects With | User Identity (ID) Management | IAC-09.1 | Mechanisms exist to ensure proper user identification management for non-consumer users and administrators. | 5 | |
| IA-04(04) | Identifier Management \| Identify User Status | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status]. | Functional | Intersects With | Identity User Status | IAC-09.2 | Mechanisms exist to identify contractors and other third-party users through unique username characteristics. | 5 | |
| IA-05(02) | Authenticator Management \| Public Key-based Authentication | a. For public key-based authentication:1. Enforce authorized access to the corresponding private key; and2. Map the authenticated identity to the account of the individual or group; andb. When public key infrastructure (PKI) is used:1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and2. Implement a local cache of revocation data to support path discovery and validation. | Functional | Equal | PKI-Based Authentication | IAC-10.2 | Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication. | 10 | |
| IA-05(06) | Authenticator Management \| Protection of Authenticators | Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. | Functional | Intersects With | User Responsibilities for Account Management | IAC-18 | Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.). | 5 | |
| IA-05(06) | Authenticator Management \| Protection of Authenticators | Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. | 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 | |
| IA-12 | Identity Proofing | a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;b. Resolve user identities to a unique individual; andc. Collect, validate, and verify identity evidence. | Functional | Equal | Identity Proofing (Identity Verification) | IAC-28 | Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions. | 10 | |
| IA-12(02) | Identity Proofing \| Identity Evidence | Require evidence of individual identification be presented to the registration authority. | Functional | Equal | Identity Evidence | IAC-28.2 | Mechanisms exist to require evidence of individual identification to be presented to the registration authority. | 10 | |
| IA-12(03) | Identity Proofing \| Identity Evidence Validation and Verification | Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification]. | Functional | Equal | Identity Evidence Validation & Verification | IAC-28.3 | Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification. | 10 | |
| IA-12(05) | Identity Proofing \| Address Confirmation | Require that a [Selection (one): registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record. | Functional | Equal | Address Confirmation | IAC-28.5 | Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital). | 10 | |
| IR-03 | Incident Response Testing | Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests]. | Functional | Intersects With | Incident Response Testing | IRO-06 | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities. | 5 | |
| IR-03(02) | Incident Response Testing \| Coordination with Related Plans | Coordinate incident response testing with organizational elements responsible for related plans. | Functional | Equal | Coordination with Related Plans | IRO-06.1 | Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans. | 10 | |
| IR-04(01) | Incident Handling \| Automated Incident Handling Processes | Support the incident handling process using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automated Incident Handling Processes | IRO-02.1 | Automated mechanisms exist to support the incident handling process. | 10 | |
| IR-06(01) | Incident Reporting \| Automated Reporting | Report incidents using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automated Reporting | IRO-10.1 | Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents. | 10 | |
| IR-06(03) | Incident Reporting \| Supply Chain Coordination | Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident. | Functional | Intersects With | Supply Chain Coordination | IRO-10.4 | Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to | 5 | |
| IR-07(01) | Incident Response Assistance \| Automation Support for Availability of Information and Support | Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automation Support of Availability of Information / Support | IRO-11.1 | Automated mechanisms exist to increase the availability of incident response-related information and support. | 10 | |
| MA-03 | Maintenance Tools | a. Approve, control, and monitor the use of system maintenance tools; andb. Review previously approved system maintenance tools [Assignment: organization-defined frequency]. | Functional | Intersects With | Maintenance Tools | MNT-04 | Mechanisms exist to control and monitor the use of system maintenance tools. | 5 | |
| MA-03(01) | Maintenance Tools \| Inspect Tools | Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications. | Functional | Equal | Inspect Tools | MNT-04.1 | Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. | 10 | |
| MA-03(02) | Maintenance Tools \| Inspect Media | Check media containing diagnostic and test programs for malicious code before the media are used in the system. | 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 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| MA-03(03) | Maintenance Tools \| Prevent Unauthorized Removal | Prevent the removal of maintenance equipment containing organizational information by:a. Verifying that there is no organizational information contained on the equipment;b. Sanitizing or destroying the equipment;c. Retaining the equipment within the facility; ord. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility. | Functional | Equal | Prevent Unauthorized Removal | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information. | 10 | |
| MA-06 | Timely Maintenance | Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure. | Functional | Equal | Timely Maintenance | MNT-03 | Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO). | 10 | |
| MP-03 | Media Marking | a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas]. | Functional | Intersects With | 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. | 5 | |
| MP-03 | Media Marking | a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas]. | Functional | Intersects With | Automated Marking | DCH-04.1 | Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies. | 5 | |
| MP-04 | Media Storage | a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; andb. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | Functional | Equal | Media Storage | DCH-06 | Mechanisms exist to:<br>(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and<br>(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 10 | |
| MP-05 | Media Transport | a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];b. Maintain accountability for system media during transport outside of controlled areas;c. Document activities associated with the transport of system media; andd. Restrict the activities associated with the transport of system media to authorized personnel. | 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 | |
| PE-04 | Access Control for Transmission | Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls]. | Functional | Equal | 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. | 10 | |
| PE-05 | Access Control for Output Devices | Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output. | Functional | Equal | 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. | 10 | |
| PE-06(01) | Monitoring Physical Access \| Intrusion Alarms and Surveillance Equipment | Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment. | Functional | Equal | Intrusion Alarms / Surveillance Equipment | PES-05.1 | Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment. | 10 | |
| PE-09 | Power Equipment and Cabling | Protect power equipment and power cabling for the system from damage and destruction. | Functional | Equal | Supporting Utilities | PES-07 | Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction. | 10 | |
| PE-10 | Emergency Shutoff | a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations;b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; andc. Protect emergency power shutoff capability from unauthorized activation. | Functional | Equal | Emergency Shutoff | PES-07.2 | Facility security mechanisms exist to shut off power in emergency situations by:<br>(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and<br>(2) Protecting emergency power shutoff capability from unauthorized activation. | 10 | |
| PE-11 | Emergency Power | Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss. | Functional | Intersects With | Emergency Power | PES-07.3 | Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source. | 5 | |
| PE-13(01) | Fire Protection \| Detection Systems — Automatic Activation and Notification | Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire. | Functional | Equal | Fire Detection Devices | PES-08.1 | Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire. | 10 | |
| PE-17 | Alternate Work Site | a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];c. Assess the effectiveness of controls at alternate work sites; andd. Provide a means for employees to communicate with information security and privacy personnel in case of incidents. | Functional | Equal | Alternate Work Site | PES-11 | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites. | 10 | |
| PL-08 | Security and Privacy Architectures | system that:1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;3. Describe how the architectures are integrated into and support the enterprise architecture; and4. Describe any assumptions about, and dependencies on, external systems and services;b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; andc. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and | Functional | Intersects With | Alignment With Enterprise Architecture | SEA-02 | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 5 | |
| RA-05(05) | Vulnerability Monitoring and Scanning \| Privileged Access | Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities]. | Functional | Equal | Privileged Access | VPM-06.3 | Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities. | 10 | |
| RA-09 | Criticality Analysis | Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]. | Functional | Intersects With | Third-Party Criticality Assessments | TPM-02 | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the | 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 | Notes |
|---|---|---|---|---|---|---|---|---|---|
| RA-09 | Criticality Analysis | Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]. | Functional | Intersects With | Criticality Analysis During Development | TDA-06.1 | Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC). | 5 | |
| RA-09 | Criticality Analysis | Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]. | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-05 | Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle | 5 | |
| SA-04(01) | Acquisition Process \| Functional Properties of Controls | Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented. | Functional | Intersects With | Functional Properties | TDA-04.1 | Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to | 5 | |
| SA-04(01) | Acquisition Process \| Functional Properties of Controls | Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented. | Functional | Intersects With | 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 | |
| SA-04(02) | Acquisition Process \| Design and Implementation Information for Controls | Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail]. | Functional | Intersects With | 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 | |
| SA-04(02) | Acquisition Process \| Design and Implementation Information for Controls | Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail]. | Functional | Intersects With | Access to Program Source Code | TDA-20 | Mechanisms exist to limit privileges to change software resident within software libraries. | 5 | |
| SA-04(02) | Acquisition Process \| Design and Implementation Information for Controls | Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail]. | Functional | Intersects With | Functional Properties | TDA-04.1 | Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to | 5 | |
| SA-04(09) | Acquisition Process \| Functions, Ports, Protocols, and Services in Use | Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use. | Functional | Equal | Ports, Protocols & Services In Use | TDA-02.1 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use. | 10 | |
| SA-09(02) | External System Services \| Identification of Functions, Ports, Protocols, and Services | Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services]. | Functional | Equal | External Connectivity Requirements - Identification of Ports, Protocols & Services | TPM-04.2 | Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications | 10 | |
| SA-10 | Developer Configuration Management | Require the developer of the system, system component, or system service to:a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];c. Implement only organization-approved changes to the system, component, or service;d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; ande. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel] | Functional | Equal | Developer Configuration Management | TDA-14 | Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation. | 10 | |
| SA-11 | Developer Testing and Evaluation | Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:a. Develop and implement a plan for ongoing security and privacy control assessments;b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;d. Implement a verifiable flaw remediation process; ande. Correct flaws identified during testing and evaluation. | Functional | Equal | Security, Compliance & Resilience Testing Throughout Development | TDA-09 | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and<br>(3) Document the results. | 10 | |
| SA-15 | Development Process, Standards, and Tools | a. Require the developer of the system, system component, or system service to follow a documented development process that:1. Explicitly addresses security and privacy requirements;2. Identifies the standards and tools used in the development process;3. Documents the specific tool options and tool configurations used in the development process; and4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; andb. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements]. | Functional | Equal | Secure Software Development Practices (SSDP) | TDA-06 | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP). | 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 |
|---|---|---|---|---|---|---|---|---|---|
| SA-15(03) | Development Process, Standards, and Tools \| Criticality Analysis | Require the developer of the system, system component, or system service to perform a criticality analysis:a. At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; andb. At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis]. | Functional | Equal | Criticality Analysis During Development | TDA-06.1 | Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC). | 10 | |
| SC-02 | Separation of System and User Functionality | Separate user functionality, including user interface services, from system management functionality. | Functional | Equal | Application Partitioning | SEA-03.2 | Mechanisms exist to separate user functionality from system management functionality. | 10 | |
| SC-04 | Information in Shared System Resources | 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 | |
| SC-07(03) | Boundary Protection \| Access Points | Limit the number of external network connections to the system. | Functional | Equal | Limit Network Connections | NET-03.1 | Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS). | 10 | |
| SC-07(04) | Boundary Protection \| External Telecommunications Services | a. Implement a managed interface for each external telecommunication service;b. Establish a traffic flow policy for each managed interface;c. Protect the confidentiality and integrity of the information being transmitted across each interface;d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;f. Prevent unauthorized exchange of control plane traffic with external networks;g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; andh. Filter unauthorized control plane traffic from external networks. | Functional | Intersects With | External Telecommunications Services | NET-03.2 | Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface. | 5 | |
| SC-07(05) | Boundary Protection \| Deny by Default — Allow by Exception | Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]]. | Functional | Intersects With | Deny Traffic by Default & Allow Traffic by Exception | NET-04.1 | Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). | 5 | |
| SC-07(07) | Boundary Protection \| Split Tunneling for Remote Devices | Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards]. | 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 | |
| SC-07(08) | Boundary Protection \| Route Traffic to Authenticated Proxy Servers | Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. | Functional | Intersects With | Route Internal Traffic to Proxy Servers | NET-18.1 | Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces. | 5 | |
| SC-07(08) | Boundary Protection \| Route Traffic to Authenticated Proxy Servers | Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. | 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 | |
| SC-08 | Transmission Confidentiality and Integrity | Protect the [Selection (one or more): confidentiality; integrity] of transmitted information. | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| SC-08 | Transmission Confidentiality and Integrity | Protect the [Selection (one or more): confidentiality; integrity] of transmitted information. | Functional | Intersects With | Transmission Integrity | CRY-04 | Cryptographic mechanisms exist to protect the integrity of data being transmitted. | 5 | |
| SC-08(01) | Transmission Confidentiality and Integrity \| Cryptographic Protection | Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission. | 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 | |
| SC-08(01) | Transmission Confidentiality and Integrity \| Cryptographic Protection | Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission. | Functional | Intersects With | 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 | |
| SC-08(01) | Transmission Confidentiality and Integrity \| Cryptographic Protection | Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission. | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| SC-10 | Network Disconnect | Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time 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 | |
| SC-17 | Public Key Infrastructure Certificates | a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; andb. Include only approved trust anchors in trust stores or certificate stores managed by the organization. | 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 | |
| SC-18 | Mobile Code | a. Define acceptable and unacceptable mobile code and mobile code technologies; andb. Authorize, monitor, and control the use of mobile code within the system. | Functional | Intersects With | Mobile Code | END-10 | Mechanisms exist to address mobile code / operating system-independent applications. | 5 | |
| SC-23 | Session Authenticity | Protect the authenticity of communications sessions. | Functional | Equal | Session Integrity | NET-09 | Mechanisms exist to protect the authenticity and integrity of communications sessions. | 10 | |
| SC-28 | Protection of Information at Rest | Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest]. | Functional | Intersects With | Endpoint Protection Measures | END-02 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 5 | |
| SC-28 | Protection of Information at Rest | Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest]. | Functional | Intersects With | Encrypting Data At Rest | CRY-05 | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest. | 5 | |
| SC-28(01) | Protection of Information at Rest \| Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | Functional | Intersects With | Cryptographic Protection | BCD-11.4 | Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information. | 5 | |
| SC-28(01) | Protection of Information at Rest \| Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | Functional | Intersects With | Encrypting Data At Rest | CRY-05 | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest. | 5 | |
| SC-28(01) | Protection of Information at Rest \| Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | Functional | Intersects With | Transmission Integrity | CRY-04 | Cryptographic mechanisms exist to protect the integrity of data being transmitted. | 5 | |
| SC-28(01) | Protection of Information at Rest \| Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | Functional | Intersects With | Encrypting Data In Storage Media | DCH-07.2 | Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. | 5 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| SI-02(02) | Flaw Remediation \| Automated Flaw Remediation Status | Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]. | Functional | Intersects With | Automated Remediation Status | VPM-05.2 | Automated mechanisms exist to determine the state of system components with regard to flaw remediation. | 5 | |
| SI-04(02) | System Monitoring \| Automated Tools and Mechanisms for Real-time Analysis | Employ automated tools and mechanisms to support near real-time analysis of events. | Functional | Equal | Automated Tools for Real-Time Analysis | MON-01.2 | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation. | 10 | |
| SI-04(04) | System Monitoring \| Inbound and Outbound Communications Traffic | a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions]. | Functional | Equal | Inbound & Outbound Communications Traffic | MON-01.3 | Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. | 10 | |
| SI-04(05) | System Monitoring \| System-generated Alerts | Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators]. | Functional | Equal | System Generated Alerts | MON-01.4 | Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational | 10 | |
| SI-07 | Software, Firmware, and Information Integrity | a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions]. | Functional | Intersects With | Endpoint File Integrity Monitoring (FIM) | END-06 | Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings. | 5 | |
| SI-07 | Software, Firmware, and Information Integrity | a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions]. | Functional | Intersects With | Safeguarding Data Over Open Networks | NET-12 | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks. | 5 | |
| SI-07 | Software, Firmware, and Information Integrity | a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions]. | Functional | Intersects With | Input Data Validation | TDA-18 | Mechanisms exist to check the validity of information inputs. | 5 | |
| SI-07(01) | Software, Firmware, and Information Integrity \| Integrity Checks | Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]]. | Functional | Equal | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 10 | |
| SI-07(07) | Software, Firmware, and Information Integrity \| Integration of Detection and Response | Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system]. | Functional | Equal | Endpoint Detection & Response (EDR) | END-06.2 | Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents. | 10 | |
| SI-08 | Spam Protection | a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; andb. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. | Functional | Equal | Phishing & Spam Protection | END-08 | Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail. | 10 | |
| SI-08(02) | Spam Protection \| Automatic Updates | Automatically update spam protection mechanisms [Assignment: organization-defined frequency]. | Functional | Equal | Automatic Spam and Phishing Protection Updates | END-08.2 | Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices. | 10 | |
| SI-10 | Information Input Validation | Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system]. | Functional | Intersects With | Safeguarding Data Over Open Networks | NET-12 | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks. | 5 | |
| SI-10 | Information Input Validation | Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system]. | Functional | Intersects With | Input Data Validation | TDA-18 | Mechanisms exist to check the validity of information inputs. | 5 | |
| SI-11 | Error Handling | a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; andb. Reveal error messages only to [Assignment: organization-defined personnel or roles]. | Functional | Equal | Error Handling | TDA-19 | Mechanisms exist to handle error conditions by:<br>(1) Identifying potentially security-relevant error conditions;<br>(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and<br>(3) Revealing error messages only to authorized personnel. | 10 | |
| SI-16 | Memory Protection | Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls]. | Functional | Equal | Memory Protection | SEA-10 | Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution. | 10 | |
| SR-06 | Supplier Assessments and Reviews | Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency]. | Functional | Intersects With | Review of Third-Party Services | TPM-08 | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls. | 5 | |