NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.01.01E	Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or Services (TAAS).	5		AC-03(02)
03.01.01E	Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	5		AC-03(02)
03.01.02E	Non-Organizationally Owned Systems – Restricted Use	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit CUI using [Assignment: organization-defined restrictions].	Functional	Intersects With	Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.	5		AC-20(03)
03.01.03E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.01.04E	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		AC-10
03.01.04E	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Functional	Intersects With	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	5		AC-10
03.01.04E	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		AC-10
03.01.05E	Automated Monitoring and Control for Remote Access	Employ automated mechanisms to monitor and control remote access methods.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5		AC-17(01)
03.01.06E	Protection of Remote Access Mechanism Information	Protect information about remote access mechanisms from unauthorized use and disclosure.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		AC-17(06)
03.01.06E	Protection of Remote Access Mechanism Information	Protect information about remote access mechanisms from unauthorized use and disclosure.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		AC-17(06)
03.01.07E	Automated Audit Actions for Account Management	Use automated mechanisms to audit account creation, modification, enabling, disabling, and removal actions.	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(04)
03.01.07E	Automated Audit Actions for Account Management	Use automated mechanisms to audit account creation, modification, enabling, disabling, and removal actions.	Functional	Intersects With	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.	5		AC-02(04)
03.01.08E	Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		AC-02(12)
03.01.08E	Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		AC-02(12)
03.01.08E	Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		AC-02(12)
03.01.08E	Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		AC-02(12)
03.01.08E	Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		AC-02(12)
03.01.09E	Attribute-Based Access Control	a. Enforce attribute-based access control policy over defined subjects and objects. b. Control access based upon [Assignment: organization-defined attributes to assume access permissions].	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	5		AC-03(13)
03.01.10E	Object Security Attributes	Use [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	Intersects With	Object Security Attributes	NET-04.2	Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.	5		AC-04(01)
03.01.10E	Object Security Attributes	Use [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	5		AC-04(01)
03.01.11E	Role-Based Access Control	a. Enforce a role-based access control policy over defined subjects and objects. b. Control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		AC-03(07)
03.01.11E	Role-Based Access Control	a. Enforce a role-based access control policy over defined subjects and objects. b. Control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		AC-03(07)
03.01.11E	Role-Based Access Control	a. Enforce a role-based access control policy over defined subjects and objects. b. Control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	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-03(07)
03.01.12E	Physical or Logical Separation of CUI Flows	Separate CUI flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques].	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		AC-04(21)
03.01.12E	Physical or Logical Separation of CUI Flows	Separate CUI flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques].	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		AC-04(21)
03.01.13E	Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Intersects With	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	5		AC-04(06)
03.01.13E	Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	5		AC-04(06)
03.01.13E	Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Intersects With	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.	5		AC-04(06)
03.01.14E	Security Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security policy].	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	5		AC-04(08)
03.01.14E	Security Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security policy].	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AC-04(08)

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.01.14E	Security Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security policy].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		AC-04(08)
03.01.14E	Security Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security policy].	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	5		AC-04(08)
03.01.14E	Security Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security policy].	Functional	Intersects With	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.	5		AC-04(08)
03.01.15E	Data Type Identifiers	Use [Assignment: organization-defined data type identifiers] to validate data that is essential for information flow decisions when transferring CUI between security domains.	Functional	Intersects With	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.	5		AC-04(12)
03.01.16E	Decomposition Into Policy-Relevant Subcomponents	Decompose CUI into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms when transferring CUI between different security domains.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		AC-04(13)
03.01.16E	Decomposition Into Policy-Relevant Subcomponents	Decompose CUI into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms when transferring CUI between different security domains.	Functional	Intersects With	Decomposition Into Policy-Related Subcomponents	NET-04.9	Automated mechanisms exist to decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains.	5		AC-04(13)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Detection of Unsanctioned Information	NET-04.10	Automated mechanisms exist to implement security policy filters requiring fully enumerated formats that restrict data structure and content, when transferring information between different security domains.	5		AC-04(15)
03.01.17E	Detection of Unsanctioned CUI	a. Examine CUI for the presence of [Assignment: organization-defined unsanctioned information] when transferring information between different security domains. b. Prohibit the transfer of the CUI defined in 03.01.17E.a in accordance with the [Assignment: organization-defined security policy].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		AC-04(15)
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		AT-02(04) AT-02(05) AT-02(06)
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		AT-02(04) AT-02(05) AT-02(06)
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5		AT-02(04) AT-02(05) AT-02(06)
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		AT-02(04) AT-02(05) AT-02(06)
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		AT-02(04) AT-02(05) AT-02(06)

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.02.01E	Advanced Literacy and Awareness Training	a. Provide security literacy training to system users: 1. On the advanced persistent threat, 2. On recognizing suspicious communications and anomalous behavior in systems using [Assignment: organization-defined indicators of malicious code], and 3. On the cyber threat environment. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5		AT-02(04) AT-02(05) AT-02(06)
03.02.02E	Literacy and Awareness Training Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5		AT-02(01)
03.02.03E	Literacy and Awareness Training Feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined personnel].	Functional	Intersects With	Training Feedback	SAT-04.1	Mechanisms exist to: (1) Monitor individual training results; and (2) Report findings to stakeholders.	5		AT-06
03.02.04E	Anti-Counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SR-11(01)
03.02.04E	Anti-Counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components.	Functional	Intersects With	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	5		SR-11(01)
03.03.01E	Protection of Audit Record Storage in Separate Physical Systems or Components	Store audit records in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5		AU-09(02)
03.03.02E	Real-Time Alerts for Audit Processing Failures	Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].	Functional	Intersects With	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	5		AU-05(02)
03.03.02E	Real-Time Alerts for Audit Processing Failures	Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5		AU-05(02)
03.03.03E	Dual Authorization for Audit Information and Actions	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].	Functional	Intersects With	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.	5		AU-09(05)
03.03.04E	Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	5		AU-06(05)
03.04.01E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.04.02E	Automated Unauthorized Component Detection	a. Detect the presence of unauthorized or misconfigured system components using [Assignment: organization-defined automated mechanisms]. b. Take the following actions when unauthorized or misconfigured 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-06(01) CM-06(02) CM-08(03)
03.04.02E	Automated Unauthorized Component Detection	a. Detect the presence of unauthorized or misconfigured system components using [Assignment: organization-defined automated mechanisms]. b. Take the following actions when unauthorized or misconfigured 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 Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5		CM-06(01) CM-06(02) CM-08(03)
03.04.02E	Automated Unauthorized Component Detection	a. Detect the presence of unauthorized or misconfigured system components using [Assignment: organization-defined automated mechanisms]. b. Take the following actions when unauthorized or misconfigured 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	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5		CM-06(01) CM-06(02) CM-08(03)
03.04.02E	Automated Unauthorized Component Detection	a. Detect the presence of unauthorized or misconfigured system components using [Assignment: organization-defined automated mechanisms]. b. Take the following actions when unauthorized or misconfigured 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		CM-06(01) CM-06(02) CM-08(03)
03.04.02E	Automated Unauthorized Component Detection	a. Detect the presence of unauthorized or misconfigured system components using [Assignment: organization-defined automated mechanisms]. b. Take the following actions when unauthorized or misconfigured 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-06(01) CM-06(02) CM-08(03)
03.04.03E	Automated Maintenance of System Component Inventory	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5		CM-08(02)
03.04.04E	Automation Support for Baseline Configuration	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5		CM-02(02)
03.04.04E	Automation Support for Baseline Configuration	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5		CM-02(02)
03.04.05E	Dual Authorization for System Changes	Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].	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		CM-05(04)
03.04.06E	Retention of Previous Configurations	Retain [Assignment: organization-defined number] previous versions of baseline configurations of the system to support rollback.	Functional	Intersects With	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	5		CM-02(03)
03.04.06E	Retention of Previous Configurations	Retain [Assignment: organization-defined number] previous versions of baseline configurations of the system to support rollback.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		CM-02(03)
03.04.07E	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(02)
03.04.07E	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)
03.04.08E	Centralized Repository	Provide a centralized repository for the inventory of system components.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5		CM-08(07)
03.05.01E	Cryptographic Bidirectional Authentication	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a system connection using bidirectional authentication that is cryptographically based.	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-03(01)

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.05.01E	Cryptographic Bidirectional Authentication	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a system connection using bidirectional authentication that is cryptographically based.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		IA-03(01)
03.05.02E	Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords. b. Protect the passwords using [Assignment: organization-defined safeguards].	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IA-05(18)
03.05.02E	Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords. b. Protect the passwords using [Assignment: organization-defined safeguards].	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5		IA-05(18)
03.05.02E	Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords. b. Protect the passwords using [Assignment: organization-defined safeguards].	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-05(18)
03.05.02E	Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords. b. Protect the passwords using [Assignment: organization-defined safeguards].	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5		IA-05(18)
03.05.03E	Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	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-03(04)
03.05.03E	Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Device Attestation	IAC-04.1	Mechanisms exist to ensure device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration management process.	5		IA-03(04)
03.05.04E	No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	5		IA-05(07)
03.05.05E	Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		IA-05(13)
03.05.05E	Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	Functional	Intersects With	Expiration of Cached Authenticators	IAC-10.10	Automated mechanisms exist to prohibit the use of cached authenticators after organization-defined time period.	5		IA-05(13)
03.05.06E	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5		IA-12
03.05.07E	Identity Providers and Authorization Servers	Employ identity providers and authorization servers to manage user, device, and non-person entity identities, attributes, and access rights that support authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		IA-13
03.05.07E	Identity Providers and Authorization Servers	Employ identity providers and authorization servers to manage user, device, and non-person entity identities, attributes, and access rights that support authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5		IA-13
03.05.07E	Identity Providers and Authorization Servers	Employ identity providers and authorization servers to manage user, device, and non-person entity identities, attributes, and access rights that support authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].	Functional	Intersects With	Identity Providers (IdP) & Authorization Servers	IAC-01.4	Mechanisms exist to employ identity providers and authorization servers to manage user, device and Non-Person Entity (NPE) identities, attributes and access rights that support authentication and authorization decisions: (1) In accordance with organization-defined identification and authentication policy; and	5		IA-13
03.06.01E	Security Operations Center	Establish and maintain a security operations center.	Functional	Intersects With	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	5		IR-04(14)
03.06.02E	Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in	Functional	Intersects With	Integrated Security Incident Response Team	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing	5		IR-04(11)
03.06.03E	Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-	5		IR-04(13)
03.06.03E	Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		IR-04(13)
03.06.04E	Automated Tracking, Data Collection, and Analysis for Incident Monitoring	Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Tracking, Data Collection & Analysis	IRO-09.1	Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data protection incidents.	5		IR-05(01)
03.07.01E	Software Updates and Patches for Maintenance Tools	Inspect maintenance tools to ensure the latest software updates and patches are installed.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5		MA-03(06)
03.08.01E	Dual Authorization for Media Sanitization	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media containing CUI].	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or	5		MP-06(07)
03.08.01E	Dual Authorization for Media Sanitization	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media containing CUI].	Functional	Intersects With	Dual Authorization for Sensitive Data Destruction	DCH-09.5	Mechanisms exist to enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive and/or regulated data.	5		MP-06(07)
03.08.02E	Dual Authorization for System Backup Deletion and Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined system backup information].	Functional	Intersects With	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.	5		CP-09(07)
03.08.02E	Dual Authorization for System Backup Deletion and Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined system backup information].	Functional	Intersects With	Dual Authorization for Sensitive Data Destruction	DCH-09.5	Mechanisms exist to enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive and/or regulated data.	5		CP-09(07)
03.08.03E	Testing System Backups for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Functional	Intersects With	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.	5		CP-09(01)
03.08.03E	Testing System Backups for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		CP-09(01)
03.08.04E	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations	5		CP-10
03.08.04E	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		CP-10
03.08.04E	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5		CP-10
03.09.01E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.09.02E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.09.03E	Access Agreements	a. Develop and document access agreements for systems processing, storing, or transmitting CUI.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5		PS-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.09.03E	Access Agreements	a. Develop and document access agreements for systems processing, storing, or transmitting CUI. b. Review and update the access agreements [Assignment: organization-defined frequency]. c. Verify that individuals requiring access to CUI and systems processing, storing, or transmitting CUI: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5		PS-06
03.09.03E	Access Agreements	a. Develop and document access agreements for systems processing, storing, or transmitting CUI. b. Review and update the access agreements [Assignment: organization-defined frequency]. c. Verify that individuals requiring access to CUI and systems processing, storing, or transmitting CUI: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		PS-06
03.09.04E	Citizenship Requirements	Verify that individuals accessing a system that processes, stores, or transmits CUI meet [Assignment: organization-defined citizenship requirements].	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5		PS-03(04)
03.09.04E	Citizenship Requirements	Verify that individuals accessing a system that processes, stores, or transmits CUI meet [Assignment: organization-defined citizenship requirements].	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for	5		PS-03(04)
03.10.01E	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		PE-06(01)
03.10.01E	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5		PE-06(01)
03.10.01E	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5		PE-06(01)
03.10.01E	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Intersects With	Monitoring Physical Access To Critical	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive and/or regulated data, in addition to the	5		PE-06(01)
03.10.01E	Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5		PE-06(01)
03.10.02E	Delivery and Removal of System Components	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility. b. Maintain records of the system components.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5		PE-16
03.10.02E	Delivery and Removal of System Components	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility. b. Maintain records of the system components.	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5		PE-16
03.11.01E	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures,	5		PM-16
03.11.02E	Threat Hunting	a. Establish and maintain a cyber threat-hunting capability to: 1. Search for indicators of compromise in organizational systems and 2. Detect, track, and disrupt threats that evade existing safeguards.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		RA-10
03.11.02E	Threat Hunting	a. Establish and maintain a cyber threat-hunting capability to: 1. Search for indicators of compromise in organizational systems and 2. Detect, track, and disrupt threats that evade existing safeguards. b. Employ the threat-hunting capability [Assignment: organization-defined frequency].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		RA-10
03.11.02E	Threat Hunting	a. Establish and maintain a cyber threat-hunting capability to: 1. Search for indicators of compromise in organizational systems and 2. Detect, track, and disrupt threats that evade existing safeguards. b. Employ the threat-hunting capability [Assignment: organization-defined frequency].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		RA-10
03.11.02E	Threat Hunting	a. Establish and maintain a cyber threat-hunting capability to: 1. Search for indicators of compromise in organizational systems and 2. Detect, track, and disrupt threats that evade existing safeguards. b. Employ the threat-hunting capability [Assignment: organization-defined frequency].	Functional	Intersects With	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		RA-10
03.11.03E	Predictive Cyber Analytics	Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].	Functional	Intersects With	Predictive Cyber Analytics	THR-01.2	Mechanisms exist to employ advanced automation and analytics capabilities to predict and identify risks to Technology Assets, Applications, Services and/or Data (TAASD).	5		RA-03(04)
03.11.04E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.11.05E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.11.06E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.11.07E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.11.08E	Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].	Functional	Intersects With	Dynamic Threat Awareness	THR-01.1	Mechanisms exist to determine and maintain ongoing awareness of the current cyber threat environment.	5		RA-03(03)
03.11.09E	Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability	5		SI-04(24)
03.11.09E	Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		SI-04(24)
03.11.09E	Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		SI-04(24)
03.11.09E	Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		SI-04(24)
03.11.10E	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:	Functional	Intersects With	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.	5		RA-09
03.11.10E	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 In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5		RA-09

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.11.10E	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 proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the	5		RA-09
03.11.10E	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
03.11.10E	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 delivery of high-value services.	5		RA-09
03.11.11E	Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		RA-05(04)
03.11.11E	Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediate	5		RA-05(04)
03.11.12E	Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		PM-16(01)
03.12.01E	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		CA-08
03.12.01E	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5		CA-08
03.12.01E	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		CA-08
03.12.02E	Independent Assessors	Use independent assessors or assessment teams to conduct security requirement assessments.	Functional	Intersects With	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.	5		CA-02(01)
03.12.03E	Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness monitoring, compliance monitoring, change monitoring.	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		CA-07(04)
03.12.03E	Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness monitoring, compliance monitoring, change monitoring.	Functional	Intersects With	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls,	5		CA-07(04)
03.12.04E	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system. b. Document, for each internal connection, the interface	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		CA-09
03.12.04E	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system. b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. c. Terminate internal system connections after [Assignment: organization-defined conditions]. d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5		CA-09
03.12.04E	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system. b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. c. Terminate internal system connections after [Assignment: organization-defined conditions]. d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	Functional	Intersects With	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	5		CA-09
03.13.01E	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		SC-29
03.13.01E	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5		SC-29
03.13.01E	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Intersects With	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	5		SC-29
03.13.02E	Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5		SC-30(02)
03.13.02E	Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Functional	Intersects With	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	5		SC-30(02)
03.13.03E	Concealment and Misdirection	Employ the following concealment and misdirection techniques to mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience	5		SC-30
03.13.03E	Concealment and Misdirection	Employ the following concealment and misdirection techniques to mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5		SC-30
03.13.04E	Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components].	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		SC-07(21)
03.13.04E	Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components].	Functional	Intersects With	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	5		SC-07(21)
03.13.05E	Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		SC-30(03)
03.13.05E	Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals].	Functional	Intersects With	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	5		SC-30(03)
03.13.06E	Platform-Independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		SC-27
03.13.06E	Platform-Independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Intersects With	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.	5		SC-27

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.13.06E	Platform-Independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		SC-27
03.13.07E	Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		SC-29(01)
03.13.07E	Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SC-29(01)
03.13.08E	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Functional	Intersects With	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	5		SC-26
03.13.09E	Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with	5		SC-07(13)
03.13.09E	Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5		SC-07(13)
03.13.10E	Separate Subnetworks	Implement separate network addresses to connect to systems in different security domains.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		SC-07(22)
03.13.11E	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		SC-25
03.13.11E	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);	5		SC-25
03.13.11E	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Thin Nodes	END-11	Mechanisms exist to configure thin nodes to have minimal functionality and information storage.	5		SC-25
03.13.12E	Denial-of-Service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events].	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		SC-05
03.13.12E	Denial-of-Service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]. b. Employ the following safeguards to prevent the denial-of-service events[Assignment: organization-defined safeguards by type of denial-of-service event].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		SC-05
03.13.12E	Denial-of-Service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]. b. Employ the following safeguards to prevent the denial-of-service events[Assignment: organization-defined safeguards by type of denial-of-service event].	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		SC-05
03.13.12E	Denial-of-Service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]. b. Employ the following safeguards to prevent the denial-of-service events[Assignment: organization-defined safeguards by type of denial-of-service event].	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		SC-05
03.13.13E	Port and Input/Output Device Access	[Selection (one): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		SC-41
03.13.13E	Port and Input/Output Device Access	[Selection (one): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.	5		SC-41
03.13.14E	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and	5		SC-44
03.13.14E	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Functional	Intersects With	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5		SC-44
03.13.15E	Separate Subnets to Isolate System Components and	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5		SC-07(29)
03.13.15E	Separate Subnets to Isolate System Components and Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		SC-07(29)
03.13.15E	Separate Subnets to Isolate System Components and Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5		SC-07(29)
03.13.16E	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);	5		SC-32
03.13.16E	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].	Functional	Intersects With	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.	5		SC-32
03.14.01E	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]. b. Take the following actions when unauthorized changes to the	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

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.14.01E	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]. b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5		SI-07
03.14.01E	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]. b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		SI-07
03.14.02E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.14.03E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.14.04E	Refresh From Trusted Sources	Obtain software and data employed during system component and service refreshes from the following trusted sources:	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	5		SI-14(01)
03.14.05E	Non-Persistent Information	a. [Selection (one): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on	Functional	Intersects With	Non-Persistent Information	SEA-08.2	Mechanisms exist to: (1) Generate or refresh information per an organization-defined frequency; and	5		SI-14(02)
03.14.06E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.14.07E	N/A	Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		N/A
03.14.08E	Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	5		SI-07(01)
03.14.08E	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	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and	5		SI-07(01)
03.14.08E	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	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		SI-07(01)
03.14.09E	Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	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		SI-07(06)
03.14.10E	Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Functional	Intersects With	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	5		SI-07(10)
03.14.10E	Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-	5		SI-07(10)
03.14.11E	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	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		SI-07(07)
03.14.11E	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	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5		SI-07(07)
03.14.11E	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	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5		SI-07(07)
03.14.11E	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	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including: (1) Endpoints;	5		SI-07(07)
03.14.12E	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-10
03.14.13E	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.	Functional	Intersects With	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for	5		SI-11
03.14.14E	Memory Protection	Implement the following safeguards to protect the system memory from unauthorized code execution: [Assignment: organization-defined safeguards].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	5		SI-16
03.14.14E	Memory Protection	Implement the following safeguards to protect the system memory from unauthorized code execution: [Assignment: organization-defined safeguards].	Functional	Intersects With	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	5		SI-16
03.14.15E	Non-Persistent System Components and Services	a. Implement non-persistent [Assignment: organization-defined system components and services]. b. Initiate non-persistent [Assignment: organization-defined	Functional	Intersects With	Applied Security, Compliance and Resilience Controls	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-	5		SI-14

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.14.15E	Non-Persistent System Components and Services	a. Implement non-persistent [Assignment: organization-defined system components and services]. b. Initiate non-persistent [Assignment: organization-defined system components and services] from a known state. c. Terminate non-persistent [Assignment: organization-defined system components and services] [Selection (one or more): upon end of session of use; [Assignment: organization-defined frequency]].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		SI-14
03.14.15E	Non-Persistent System Components and Services	a. Implement non-persistent [Assignment: organization-defined system components and services]. b. Initiate non-persistent [Assignment: organization-defined system components and services] from a known state. c. Terminate non-persistent [Assignment: organization-defined system components and services] [Selection (one or more): upon end of session of use; [Assignment: organization-defined frequency]].	Functional	Intersects With	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	5		SI-14
03.14.16E	Tainting	Embed data or capabilities in the following systems or system components to determine if CUI has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and	5		SI-20
03.14.16E	Tainting	Embed data or capabilities in the following systems or system components to determine if CUI has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	5		SI-20
03.14.17E	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	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		SI-04(05)
03.14.17E	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	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		SI-04(05)
03.14.17E	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	Intersects With	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 awareness.	5		SI-04(05)
03.14.17E	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	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5		SI-04(05)
03.14.17E	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	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		SI-04(05)
03.14.18E	Automated Organization-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security implications occur: [Assignment: organization-	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		SI-04(12)
03.14.18E	Automated Organization-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5		SI-04(12)
03.14.18E	Automated Organization-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		SI-04(12)
03.14.19E	Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5		SI-04(14)
03.15.01E	Security Architecture	a. Develop a security architecture for the system that: 1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI,	Functional	Intersects With	Applied Security, Compliance and Resilience Controls	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-	5		PL-08
03.15.01E	Security Architecture	a. Develop a security architecture for the system that: 1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI, 2. Describes how the architecture is integrated into and supports the enterprise architecture, and 3. Describes any assumptions about, and dependencies on, external systems and services. b. Review and update the security architecture [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture. c. Reflect planned security architecture changes in system security plans, concept of operations, criticality analysis, organizational procedures, and procurements and acquisitions.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		PL-08
03.15.01E	Security Architecture	a. Develop a security architecture for the system that: 1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI, 2. Describes how the architecture is integrated into and supports the enterprise architecture, and 3. Describes any assumptions about, and dependencies on, external systems and services. b. Review and update the security architecture [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture. c. Reflect planned security architecture changes in system security plans, concept of operations, criticality analysis, organizational procedures, and procurements and acquisitions.	Functional	Intersects With	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	5		PL-08
03.15.01E	Security Architecture	a. Develop a security architecture for the system that: 1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI, 2. Describes how the architecture is integrated into and supports the enterprise architecture, and 3. Describes any assumptions about, and dependencies on, external systems and services. b. Review and update the security architecture [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture. c. Reflect planned security architecture changes in system security plans, concept of operations, criticality analysis, organizational procedures, and procurements and acquisitions.	Functional	Intersects With	Security-Aware Design	SEA-01.5	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		PL-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.15.01E	Security Architecture	a. Develop a security architecture for the system that: 1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI, 2. Describes how the architecture is integrated into and supports the enterprise architecture, and 3. Describes any assumptions about, and dependencies on, external systems and services. b. Review and update the security architecture [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture. c. Reflect planned security architecture changes in system security plans, concept of operations, criticality analysis, organizational procedures, and procurements and acquisitions.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		PL-08
03.15.02E	Defense In Depth	a. Design the security architecture for the system using a defense-in-depth approach. b. Allocate [Assignment: organization-defined security requirements] to [Assignment: organization-defined architectural layers and locations]. c. Ensure that the allocated requirements operate in a coordinated and mutually reinforcing manner.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		PL-08(01)
03.15.02E	Defense In Depth	a. Design the security architecture for the system using a defense-in-depth approach. b. Allocate [Assignment: organization-defined security requirements] to [Assignment: organization-defined architectural layers and locations]. c. Ensure that the allocated requirements operate in a coordinated and mutually reinforcing manner.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5		PL-08(01)
03.15.03E	Supplier Diversity	Require that [Assignment: organization-defined safeguards] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		PL-08(02)
03.15.03E	Supplier Diversity	Require that [Assignment: organization-defined safeguards] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5		PL-08(02)
03.16.01E	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission-essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		SA-23
03.16.01E	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission-	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5		SA-23
03.16.01E	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission-essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5		SA-23
03.17.01E	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		SR-08
03.17.01E	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5		SR-08
03.17.02E	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; [Assignment: organization-defined frequency]; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5		SR-10
03.17.02E	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; [Assignment: organization-defined frequency]; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5		SR-10
03.17.02E	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; [Assignment: organization-defined frequency]; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and	5		SR-10
03.17.02E	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; [Assignment: organization-defined frequency]; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		SR-10

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST SP 800 - 172 R3 - Enhanced Security Requirements for Protecting Controlled Unclassified Information
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/172/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST 800-53 R5
03.17.02E	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; [Assignment: organization-defined frequency]; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		SR-10
03.17.03E	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		SR-11
03.17.03E	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		SR-11
03.17.03E	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5		SR-11
03.17.03E	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		SR-11
03.17.04E	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated CUI: [Assignment: organization-defined systems, system components, and associated CUI].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		SR-04
03.17.05E	Supply Chain Integrity – Pedigree	Employ [Assignment: organization-defined safeguards] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5		SR-04(04)
03.17.05E	Supply Chain Integrity – Pedigree	Employ [Assignment: organization-defined safeguards] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components	5		SR-04(04)
03.17.05E	Supply Chain Integrity – Pedigree	Employ [Assignment: organization-defined safeguards] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		SR-04(04)