**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| 03.01.01E | Dual Authorization | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.01E | Dual Authorization | dual authorization is enforced for <A.03.01.01E.ODP[01]: privileged commands and/or other 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 | |
| DS-A.03.01.01E | Dual Authorization | dual authorization is enforced for <A.03.01.01E.ODP[01]: privileged commands and/or other actions>. | Functional | Intersects With | Dual Authorization for Privileged Commands | IAC-20.5 | Automated mechanisms exist to enforce dual authorization for privileged commands. | 5 | |
| A.03.01.01E.ODP[01] | Dual Authorization | privileged commands and/or other actions requiring dual authorization are defined. | 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 | |
| A.03.01.01E.ODP[01] | Dual Authorization | privileged commands and/or other actions requiring dual authorization are defined. | Functional | Intersects With | Dual Authorization for Privileged Commands | IAC-20.5 | Automated mechanisms exist to enforce dual authorization for privileged commands. | 5 | |
| 03.01.02E | Non-Organizationally Owned Systems - Restricted Use | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.02E | Non-Organizationally Owned Systems - Restricted Use | the use of non-organizationally owned systems or system components to process, store, or transmit CUI is restricted using <A.03.01.02E.ODP[01]: 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 | |
| A.03.01.02E.ODP[01] | Non-Organizationally Owned Systems - Restricted Use | restrictions on the use of non-organizationally owned systems or system components to process, store, or transmit CUI are defined. | 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 | |
| 03.01.03E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.01.04E | Concurrent Session Control | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.04E | Concurrent Session Control | the number of concurrent sessions for each <A.03.01.04E.ODP[01]: account and/or account types> is limited to <A.03.01.04E.ODP[02]: number>. | Functional | Intersects With | Concurrent Session Control | IAC-23 | Mechanisms exist to limit the number of concurrent sessions for each system account. | 5 | |
| A.03.01.04E.ODP[01] | Concurrent Session Control | accounts and/or account types for which to limit the number of concurrent sessions is defined. | 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 | |
| A.03.01.04E.ODP[01] | Concurrent Session Control | accounts and/or account types for which to limit the number of concurrent sessions is defined. | Functional | Intersects With | Concurrent Session Control | IAC-23 | Mechanisms exist to limit the number of concurrent sessions for each system account. | 5 | |
| A.03.01.04E.ODP[02] | Concurrent Session Control | the number of concurrent sessions to be allowed for each account and/or account type is defined. | Functional | Intersects With | Concurrent Session Control | IAC-23 | Mechanisms exist to limit the number of concurrent sessions for each system account. | 5 | |
| A.03.01.04E.ODP[02] | Concurrent Session Control | the number of concurrent sessions to be allowed for each account and/or account type is defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.01.05E | Automated Monitoring and Control for Remote Access | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.05E[01] | Automated Monitoring and Control for Remote Access | automated mechanisms are employed to monitor remote access methods. | Functional | Intersects With | Automated Monitoring & Control | NET-14.1 | Automated mechanisms exist to monitor and control remote access sessions. | 5 | |
| DS-A.03.01.05E[02] | Automated Monitoring and Control for Remote Access | automated mechanisms are employed to control remote access methods. | Functional | Intersects With | Automated Monitoring & Control | NET-14.1 | Automated mechanisms exist to monitor and control remote access sessions. | 5 | |
| 03.01.06E | Protection of Remote Access Mechanism Information | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.06E | Protection of Remote Access Mechanism Information | information about remote access mechanisms is protected 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| DS-A.03.01.06E | Protection of Remote Access Mechanism Information | information about remote access mechanisms is protected 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 | |
| 03.01.07E | Automated Audit Actions for Account Management | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.07E[01] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account creation 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 | |
| DS-A.03.01.07E[01] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account creation 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 | |
| DS-A.03.01.07E[02] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account modification 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 | |
| DS-A.03.01.07E[02] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account modification 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 | |
| DS-A.03.01.07E[03] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account enabling 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 | |
| DS-A.03.01.07E[03] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account enabling 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 | |
| DS-A.03.01.07E[04] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account disabling 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 | |
| DS-A.03.01.07E[04] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account disabling 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 | |
| DS-A.03.01.07E[05] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account 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 | |
| DS-A.03.01.07E[05] | Automated Audit Actions for Account Management | automated mechanisms are used to audit account 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 | |
| 03.01.08E | Account Monitoring for Atypical Usage | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.08E.a | Account Monitoring for Atypical Usage | system accounts are monitored for <A.03.01.08E.ODP[01]: atypical usage>. | 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 | |
| DS-A.03.01.08E.a | Account Monitoring for Atypical Usage | system accounts are monitored for <A.03.01.08E.ODP[01]: atypical usage>. | 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 | |
| A.03.01.08E.ODP[01] | Account Monitoring for Atypical Usage | atypical usage for which to monitor system accounts is defined. | 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 | |
| DS-A.03.01.08E.b | Account Monitoring for Atypical Usage | atypical usage of system accounts is reported to <A.03.01.08E.ODP[02]: 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 | |
| A.03.01.08E.ODP[02] | Account Monitoring for Atypical Usage | personnel or roles to report atypical usage are defined. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| 03.01.09E | Attribute-Based Access Control | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.09E.a[01] | Attribute-Based Access Control | the attribute-based access control policy is enforced over defined subjects. | 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 | |
| DS-A.03.01.09E.a[02] | Attribute-Based Access Control | the attribute-based access control policy is enforced over defined objects. | 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 | |
| DS-A.03.01.09E.b | Attribute-Based Access Control | access is controlled based upon <A.03.01.09E.ODP[01]: attributes>. | 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 | |
| A.03.01.09E.ODP[01] | Attribute-Based Access Control | attributes to assume access permissions are defined. | 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 | |
| 03.01.10E | Object Security Attributes | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.10E | Object Security Attributes | <A.03.01.10E.ODP[01]: security attributes> associated with <A.03.01.10E.ODP[02]: information objects>, <A.03.01.10E.ODP[03]: source objects>, and <A.03.01.10E.ODP[04]: destination objects> are used to enforce <A.03.01.10E.ODP[05]: 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 | |
| A.03.01.10E.ODP[01] | Object Security Attributes | security attributes to be associated with information, source, and destination objects are defined. | 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 | |
| A.03.01.10E.ODP[02] | Object Security Attributes | information objects to be associated with information security attributes are defined. | 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 | |
| A.03.01.10E.ODP[03] | Object Security Attributes | source objects to be associated with information security attributes are defined. | 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 | |
| A.03.01.10E.ODP[04] | Object Security Attributes | destination objects to be associated with information security attributes are defined. | 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 | |
| A.03.01.10E.ODP[05] | Object Security Attributes | information flow control policies as a basis for the enforcement of flow control decisions are defined. | 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 | |
| 03.01.11E | Role-Based Access Control | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.11E.a | Role-Based Access Control | a role-based access control policy over defined subjects and objects is enforced. | 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 | |
| DS-A.03.01.11E.a | Role-Based Access Control | a role-based access control policy over defined subjects and objects is enforced. | 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 | |
| DS-A.03.01.11E.b | Role-Based Access Control | access is controlled based upon <A.03.01.11E.ODP[01] roles and authorized users>. | 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 | |
| A.03.01.11E.ODP[01] | Role-Based Access Control | roles and users authorized to assume such roles are defined. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| 03.01.12E | Physical or Logical Separation of CUI Flows | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.12E | Physical or Logical Separation of CUI Flows | CUI flows are logically or physically separated using <A.03.01.12E.ODP[01] 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 | |
| A.03.01.12E.ODP[01] | Physical or Logical Separation of CUI Flows | mechanisms and/or techniques to separate CUI flows are defined. | 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 | |
| A.03.01.12E.ODP[01] | Physical or Logical Separation of CUI Flows | mechanisms and/or techniques to separate CUI flows are defined. | 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 | |
| 03.01.13E | Metadata | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.13E | Metadata | information flow control based on <A.03.01.13E.ODP[01]: metadata> is enforced. | 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 | |
| DS-A.03.01.13E | Metadata | information flow control based on <A.03.01.13E.ODP[01]: metadata> is enforced. | 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 | |
| A.03.01.13E.ODP[01] | Metadata | metadata that requires flow control is defined. | Functional | Intersects With | Metadata | NET-04.5 | Mechanisms exist to enforce information flow controls based on metadata. | 5 | |
| 03.01.14E | Security Policy Filters | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.14E.a | Security Policy Filters | information flow control is enforced using <A.03.01.14E.ODP[01] security policy filters> as a basis for flow control decisions for <A.03.01.14E.ODP[02] information flows>. | 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 | |
| DS-A.03.01.14E.a | Security Policy Filters | information flow control is enforced using <A.03.01.14E.ODP[01] security policy filters> as a basis for flow control decisions for <A.03.01.14E.ODP[02] information flows>. | 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 | |
| A.03.01.14E.ODP[01] | Security Policy Filters | security policy filers are defined. | 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 | |
| A.03.01.14E.ODP[02] | Security Policy Filters | information flows are defined. | 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 | |
| A.03.01.14E.ODP[02] | Security Policy Filters | information flows are defined. | Functional | Intersects With | Network Diagrams & Data Flow Diagrams (DFDs) | AST-04 | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive and/or regulated data flows. | 5 | |
| DS-A.03.01.14E.b | Security Policy Filters | <A.03.01.14E.ODP[03]: SELECTED PARAMETER VALUE(S)> data after a filter processing failure in accordance with <A.03.01.14E.ODP[04] 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 | |
| A.03.01.14E.ODP[03] | Security Policy Filters | one or more of the following PARAMETER VALUES is/are selected: {Block; Strip; Modify; Quarantine} in response to a filter processing failure. | 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 | |
| A.03.01.14E.ODP[04] | Security Policy Filters | security policy addressing a filter processing failure is defined. | 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 | |
| 03.01.15E | Data Type Identifiers | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.15E | Data Type Identifiers | when transferring information between security domains, <A.03.01.15E.ODP[01]: data type identifiers> are used to validate data that is essential for information flow decisions. | 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 | |
| A.03.01.15E.ODP[01] | Data Type Identifiers | data type identifiers are defined. | 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 | |
| 03.01.16E | Decomposition Into Policy-Relevant Subcomponents | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.16E | Decomposition Into Policy-Relevant Subcomponents | when transferring information between different security domains, CUI is decomposed into <A.03.01.16E.ODP[01]: policy-relevant subcomponents> for submission to policy enforcement mechanisms | 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 | |
| A.03.01.16E.ODP[01] | Decomposition Into Policy-Relevant Subcomponents | policy-relevant subcomponents into which to decompose information for submission to policy enforcement mechanisms are defined. | 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| 03.01.17E | Detection of Unsanctioned CUI | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.01.17E.a | Detection of Unsanctioned CUI | when transferring information between different security domains, information is examined for the presence of <A.03.01.17E.ODP[01] unsanctioned information>. | 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 | |
| DS-A.03.01.17E.a | Detection of Unsanctioned CUI | when transferring information between different security domains, information is examined for the presence of <A.03.01.17E.ODP[01] unsanctioned information>. | 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 | |
| A.03.01.17E.ODP[01] | Detection of Unsanctioned CUI | unsanctioned information to be detected is defined. | 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 | |
| DS-A.03.01.17E.b | Detection of Unsanctioned CUI | the transfer of CUI defined in 03.01.17E.a is prohibited in accordance with <A.03.01.17E.ODP[02] 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 | |
| A.03.01.17E.ODP[02] | Detection of Unsanctioned CUI | a security policy that prohibits the transfer of such information is defined. | 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 | |
| A.03.01.17E.ODP[02] | Detection of Unsanctioned CUI | a security policy that prohibits the transfer of such information is defined. | Functional | Intersects With | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 5 | |
| A.03.01.17E.ODP[02] | Detection of Unsanctioned CUI | a security policy that prohibits the transfer of such information is defined. | 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 | |
| A.03.01.17E.ODP[02] | Detection of Unsanctioned CUI | a security policy that prohibits the transfer of such information is defined. | 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 | |
| 03.02.01E | Advanced Literacy and Awareness Training | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.02.01E.a.01 | Advanced Literacy and Awareness Training | security literacy training on the advanced persistent threat is provided to system users. | 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 | |
| DS-A.03.02.01E.a.02 | Advanced Literacy and Awareness Training | security literacy training on recognizing suspicious communications and anomalous behavior in systems using <A.03.02.01E.ODP[01]: indicators of malicious code> is provided to system users. | Functional | Intersects With | Role-Based Security, Compliance & Resilience Training | SAT-03 | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>(1) Before authorizing access to the system or performing assigned duties;<br>(2) When required by system changes; and<br>(3) Annually thereafter. | 5 | |
| DS-A.03.02.01E.a.02 | Advanced Literacy and Awareness Training | security literacy training on recognizing suspicious communications and anomalous behavior in systems using <A.03.02.01E.ODP[01]: indicators of malicious code> is provided to system users. | 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 | |
| A.03.02.01E.ODP[01] | Advanced Literacy and Awareness Training | indicators of malicious code are defined. | 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 | |
| DS-A.03.02.01E.a.03 | Advanced Literacy and Awareness Training | security literacy training on the cyber threat environment is provided to system users. | 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 | |
| DS-A.03.02.01E.b[01] | Advanced Literacy and Awareness Training | security literacy training content is updated <A.03.02.01E.ODP[02]: frequency>. | 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:<br>(1) Organizational policies, standards and procedures;<br>(2) Assigned roles and responsibilities;<br>(3) Relevant threats and risks; and<br>(4) Technological developments. | 5 | |
| A.03.02.01E.ODP[02] | Advanced Literacy and Awareness Training | the frequency at which to update security literacy training content is defined. | 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 | |
| DS-A.03.02.01E.b[02] | Advanced Literacy and Awareness Training | security literacy training content is updated following <A.03.02.01E.ODP[03]: 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:<br>(1) Organizational policies, standards and procedures;<br>(2) Assigned roles and responsibilities;<br>(3) Relevant threats and risks; and<br>(4) Technological developments. | 5 | |
| A.03.02.01E.ODP[03] | Advanced Literacy and Awareness Training | events which cause security literacy training content to be updated are defined. | 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:<br>(1) Organizational policies, standards and procedures;<br>(2) Assigned roles and responsibilities;<br>(3) Relevant threats and risks; and<br>(4) Technological developments. | 5 | |
| 03.02.02E | Literacy and Awareness Training Practical Exercises | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.02.02E | Literacy and Awareness Training Practical Exercises | practical exercises in literacy training that simulate events and incidents are provided. | 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 | |
| 03.02.03E | Literacy and Awareness Training Feedback | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.02.03E | Literacy and Awareness Training Feedback | feedback on organizational training results is provided to <A.03.02.03E.ODP[01]: personnel>. | Functional | Intersects With | Training Feedback | SAT-04.1 | Mechanisms exist to:<br>(1) Monitor individual training results; and<br>(2) Report findings to stakeholders. | 5 | |
| A.03.02.03E.ODP[01] | Literacy and Awareness Training Feedback | personnel to whom feedback on organizational training results will be provided are assigned. | Functional | Intersects With | Stakeholder Accountability Structure | GOV-04.1 | Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks. | 5 | |
| 03.02.04E | Anti-Counterfeit Training | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.02.04E | Anti-Counterfeit Training | <A.03.02.04E.ODP[01]: personnel or roles> are trained 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 | |
| A.03.02.04E.ODP[01] | Anti-Counterfeit Training | personnel or roles requiring training to detect counterfeit system components are defined. | Functional | Intersects With | Role-Based Security, Compliance & Resilience Training | SAT-03 | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>(1) Before authorizing access to the system or performing assigned duties;<br>(2) When required by system changes; and<br>(3) Annually thereafter. | 5 | |
| 03.03.01E | Protection of Audit Record Storage in Physical Systems or Components | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.03.01E | Protection of Audit Record Storage in Physical Systems or Components | audit records are stored 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 | |
| 03.03.02E | Real-Time Alerts for Audit Processing Failures | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.03.02E | Real-Time Alerts for Audit Processing Failures | an alert is provided within <A.03.03.02E.ODP[01]: real-time period> to <A.03.03.02E.ODP[02]: personnel, roles, and/or locations> when <A.03.03.02E.ODP[03]: audit logging failure events> occur. | 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 | |
| A.03.03.02E.ODP[01] | Real-Time Alerts for Audit Processing Failures | real-time period requiring alerts when audit failure events (defined in A.03.03.02E.ODP[03]) occur is defined. | 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 | |
| A.03.03.02E.ODP[03] | Real-Time Alerts for Audit Processing Failures | audit logging failure events requiring real-time alerts are defined. | 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 | |
| A.03.03.02E.ODP[02] | Real-Time Alerts for Audit Processing Failures | personnel, roles, and/or locations to be alerted in real time when audit failure events (defined in A.03.03.02E.ODP[03]) occur are defined. | 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| 03.03.03E | Dual Authorization for Audit Information and Actions | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.03.03E | Dual Authorization for Audit Information and Actions | dual authorization is enforced for the <A.03.03.03E.ODP[01]: SELECTED PARAMETER VALUE(S)> of <A.03.03.03E.ODP[02]: 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 | |
| A.03.03.03E.ODP[01] | Dual Authorization for Audit Information and Actions | one or more of the following PARAMETER VALUES is/are selected: {movement; deletion}. | 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 | |
| A.03.03.03E.ODP[02] | Dual Authorization for Audit Information and Actions | audit information for which dual authorization is to be enforced is defined. | 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 | |
| 03.03.04E | Integrated Analysis of Audit Records | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.03.04E | Integrated Analysis of Audit Records | analysis of audit records is integrated with analysis of <A.03.03.04E.ODP[01]: SELECTED PARAMETER VALUE(S)> 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 | |
| A.03.03.04E.ODP[01] | Integrated Analysis of Audit Records | one or more of the following PARAMETER VALUES is/are selected: {vulnerability scanning information; performance data; system monitoring information; <A.03.03.04E.ODP[02] data/information collected from other sources>}. | 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 | |
| A.03.03.04E.ODP[02] | Integrated Analysis of Audit Records | data or information collected from other sources to be analyzed is defined (if selected). | 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 | |
| 03.04.01E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.04.02E | Automated Unauthorized Component Detection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.02E.a | Automated Unauthorized Component Detection | the presence of unauthorized or misconfigured system components is detected using <A.03.04.02E.ODP[01]: automated mechanisms>. | 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 | |
| A.03.04.02E.ODP[01] | Automated Unauthorized Component Detection | automated mechanisms used to detect the presence of unauthorized or misconfigured system components are defined. | 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 | |
| DS-A.03.04.02E.b | Automated Unauthorized Component Detection | one or more of the following actions is/are taken when unauthorized or misconfigured system components are detected: <A.03.04.02E.ODP[02]: SELECTED PARAMETER VALUE(S)>. | Functional | Intersects With | Respond To Unauthorized Changes | CFG-02.8 | Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents. | 5 | |
| DS-A.03.04.02E.b | Automated Unauthorized Component Detection | one or more of the following actions is/are taken when unauthorized or misconfigured system components are detected: <A.03.04.02E.ODP[02]: SELECTED PARAMETER VALUE(S)>. | 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 | |
| A.03.04.02E.ODP[02] | Automated Unauthorized Component Detection | one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized or misconfigured system components; isolate unauthorized or misconfigured system components; notify <A.03.04.02E.ODP[03] 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 | |
| A.03.04.02E.ODP[03] | Automated Unauthorized Component Detection | personnel or roles to be notified when unauthorized or misconfigured system components are detected are defined (if selected). | 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 | |
| 03.04.03E | Automated Maintenance of System Component Inventory | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.03E[01] | Automated Maintenance of System Component Inventory | <A.03.04.03E.ODP[01]: automated mechanisms> are used to maintain the currency of the system component inventory. | 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 | |
| DS-A.03.04.03E[01] | Automated Maintenance of System Component Inventory | <A.03.04.03E.ODP[01]: automated mechanisms> are used to maintain the currency of the system component inventory. | 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 | |
| A.03.04.03E.ODP[01] | Automated Maintenance of System Component Inventory | automated mechanisms used to maintain the currency of the system component inventory are defined. | 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 | |
| DS-A.03.04.03E[02] | Automated Maintenance of System Component Inventory | <A.03.04.03E.ODP[02]: automated mechanisms> are used to maintain the completeness of the system component inventory. | 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 | |
| A.03.04.03E.ODP[02] | Automated Maintenance of System Component Inventory | automated mechanisms used to maintain the completeness of the system component inventory are defined. | 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 | |
| DS-A.03.04.03E[03] | Automated Maintenance of System Component Inventory | <A.03.04.03E.ODP[03]: automated mechanisms> are used to maintain the accuracy of the system component inventory. | 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 | |
| A.03.04.03E.ODP[03] | Automated Maintenance of System Component Inventory | automated mechanisms used to maintain the accuracy of the system component inventory are defined. | 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 | |
| DS-A.03.04.03E[04] | Automated Maintenance of System Component Inventory | <A.03.04.03E.ODP[04]: automated mechanisms> are used to maintain the availability of the system component inventory. | 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 | |
| A.03.04.03E.ODP[04] | Automated Maintenance of System Component Inventory | automated mechanisms used to maintain the availability of the system component inventory are defined. | 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 | |
| 03.04.04E | Automation Support for Baseline Configuration | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.04E[01] | Automation Support for Baseline Configuration | the currency of the baseline configuration of the system is maintained using <A.03.04.04E.ODP[01]: 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 | |
| A.03.04.04E.ODP[01] | Automation Support for Baseline Configuration | automated mechanisms for maintaining the baseline configuration of the system are defined. | 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 | |
| DS-A.03.04.04E[02] | Automation Support for Baseline Configuration | the completeness of the baseline configuration of the system is maintained using <A.03.04.04E.ODP[01]: 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 | |
| DS-A.03.04.04E[03] | Automation Support for Baseline Configuration | the accuracy of the baseline configuration of the system is maintained using <A.03.04.04E.ODP[01]: 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 | |
| DS-A.03.04.04E[04] | Automation Support for Baseline Configuration | the availability of the baseline configuration of the system is maintained using <A.03.04.04E.ODP[01]: 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 | |
| 03.04.05E | Dual Authorization for System Changes | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.05E[01] | Dual Authorization for System Changes | dual authorization for implementing changes to <A.03.04.05E.ODP[01]: system components> is enforced. | 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 | |
| A.03.04.05E.ODP[01] | Dual Authorization for System Changes | system components requiring dual authorization for the implementation of changes are defined. | 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 | |
| DS-A.03.04.05E[02] | Dual Authorization for System Changes | dual authorization for implementing changes to <A.03.04.05E.ODP[02]: system-level information> is enforced. | 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 | |
| A.03.04.05E.ODP[02] | Dual Authorization for System Changes | system-level information requiring dual authorization for the implementation of changes is defined. | 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| 03.04.06E | Retention of Previous Configurations | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.06E | Retention of Previous Configurations | <A.03.04.06E.ODP[01]: number> previous versions of baseline configurations of the system are retained 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 | |
| DS-A.03.04.06E | Retention of Previous Configurations | <A.03.04.06E.ODP[01]: number> previous versions of baseline configurations of the system are retained 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 | |
| A.03.04.06E.ODP[01] | Retention of Previous Configurations | the number of previous baseline configuration versions to be retained is defined. | Functional | Intersects With | Retention Of Previous Configurations | CFG-02.3 | Mechanisms exist to retain previous versions of baseline configuration to support roll back. | 5 | |
| 03.04.07E | Testing, Validation, and Documentation of Changes | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.07E[01] | Testing, Validation, and Documentation of Changes | changes to the system are tested 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 | |
| DS-A.03.04.07E[02] | Testing, Validation, and Documentation of Changes | changes to the system are validated 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 | |
| DS-A.03.04.07E[03] | Testing, Validation, and Documentation of Changes | changes to the system are documented 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 | |
| 03.04.08E | Centralized Repository | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.04.08E | Centralized Repository | a centralized repository for the inventory of system components is provided. | 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 | |
| 03.05.01E | Cryptographic Bidirectional Authentication | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.01E | Cryptographic Bidirectional Authentication | <A.03.05.01E.ODP[01]: devices and/or types of devices> are authenticated 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 | |
| A.03.05.01E.ODP[01] | Cryptographic Bidirectional Authentication | devices and/or types of devices requiring the use of cryptographically based bidirectional authentication to authenticate before establishing a system connection are defined. | 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 | |
| 03.05.02E | Password Managers | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.02E.a | Password Managers | <A.03.05.02E.ODP[01]: password managers> are employed to generate and manage passwords. | Functional | Intersects With | Password Managers | IAC-10.11 | Mechanisms exist to protect and store passwords via a password manager tool. | 5 | |
| A.03.05.02E.ODP[01] | Password Managers | password managers employed for generating and managing passwords are defined. | 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 | |
| DS-A.03.05.02E.b | Password Managers | passwords are protected using <A.03.05.02E.ODP[02]: 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 | |
| A.03.05.02E.ODP[02] | Password Managers | controls for protecting passwords are defined. | 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 | |
| 03.05.03E | Device Attestation | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.03E | Device Attestation | device identification and authentication are handled based on attestation by <A.03.05.03E.ODP[01]: 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 | |
| A.03.05.03E.ODP[01] | Device Attestation | the configuration management process to be implemented to handle device identification and authentication based on attestation is defined. | 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 | |
| 03.05.04E | No Embedded Unencrypted Static Authenticators | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.04E | No Embedded Unencrypted Static Authenticators | 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 | |
| 03.05.05E | Expiration of Cached Authenticators | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.05E | Expiration of Cached Authenticators | the use of cached authenticators is prohibited after <A.03.05.05E.ODP[01]: 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 standards. | 5 | |
| A.03.05.05E.ODP[01] | Expiration of Cached Authenticators | the time period after which the use of cached authenticators is prohibited is defined. | 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 | |
| 03.05.06E | Identity Proofing | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.06E.a | Identity Proofing | users who require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines are identity-proofed. | 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 | |
| DS-A.03.05.06E.b | Identity Proofing | user identities are resolved to a unique individual. | 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 | |
| DS-A.03.05.06E.c[01] | Identity Proofing | identity evidence is collected. | 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 | |
| DS-A.03.05.06E.c[02] | Identity Proofing | identity evidence is validated. | 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 | |
| DS-A.03.05.06E.c[03] | Identity Proofing | identity evidence is verified. | 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 | |
| 03.05.07E | Identity Providers and Authorization Servers | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.05.07E[01] | Identity Providers and Authorization Servers | identity providers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication decisions in accordance with <A.03.05.07E.ODP[01]: policy> using <A.03.05.07E.ODP[02]: 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:<br>(1) In accordance with organization-defined identification and authentication policy; and<br>(2) Using organization-defined mechanisms. | 5 | |
| A.03.05.07E.ODP[01] | Identity Providers and Authorization Servers | an identification and authentication policy is defined. | 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 | |
| A.03.05.07E.ODP[01] | Identity Providers and Authorization Servers | an identification and authentication policy is defined. | Functional | Intersects With | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 5 | |
| A.03.05.07E.ODP[02] | Identity Providers and Authorization Servers | mechanisms supporting authentication and authorization decisions are defined. | 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:<br>(1) In accordance with organization-defined identification and authentication policy; and<br>(2) Using organization-defined mechanisms. | 5 | |
| DS-A.03.05.07E[02] | Identity Providers and Authorization Servers | identity providers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authorization decisions in accordance with <A.03.05.07E.ODP[01]: policy> using <A.03.05.07E.ODP[02]: 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:<br>(1) In accordance with organization-defined identification and authentication policy; and<br>(2) Using organization-defined mechanisms. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.05.07E[03] | Identity Providers and Authorization Servers | authorization servers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication decisions in accordance with <A.03.05.07E.ODP[01]: policy> using <A.03.05.07E.ODP[02]: 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:<br>(1) In accordance with organization-defined identification and authentication policy; and<br>(2) Using organization-defined mechanisms. | 5 | |
| 03.06.01E | Security Operations Center | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.06.01E[01] | Security Operations Center | a security operations center is established. | 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 | |
| DS-A.03.06.01E[02] | Security Operations Center | a security operations center is maintained. | 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 | |
| 03.06.02E | Integrated Incident Response Team | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.06.02E[01] | Integrated Incident Response Team | an integrated incident response team is established. | Functional | Intersects With | Integrated Security Incident Response Team (ISIRT) | IRO-07 | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations. | 5 | |
| A.03.06.02E.ODP[01] | Integrated Incident Response Team | the time period within which an integrated incident response team can be deployed is defined. | Functional | Intersects With | Integrated Security Incident Response Team (ISIRT) | IRO-07 | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations. | 5 | |
| DS-A.03.06.02E[02] | Integrated Incident Response Team | an integrated incident response team is maintained. | Functional | Intersects With | Integrated Security Incident Response Team (ISIRT) | IRO-07 | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations. | 5 | |
| DS-A.03.06.02E[03] | Integrated Incident Response Team | the integrated incident response team can be deployed to any location identified by the organization in <A.03.06.02E.ODP[01]: time period>. | Functional | Intersects With | Integrated Security Incident Response Team (ISIRT) | IRO-07 | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations. | 5 | |
| 03.06.03E | Behavior Analysis | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.06.03E | Behavior Analysis | anomalous or suspected adversarial behavior in or related to <A.03.06.03E.ODP[01]: environments or resources> is analyzed. | 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 | |
| A.03.06.03E.ODP[01] | Behavior Analysis | environments or resources that may contain or be related to anomalous or suspected adversarial behavior are defined. | 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-parties). | 5 | |
| 03.06.04E | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.06.04E[01] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | incidents are tracked using <A.03.06.04E.ODP[01]: 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 | |
| A.03.06.04E.ODP[01] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | automated mechanisms used to track incidents are defined. | 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 | |
| DS-A.03.06.04E[02] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | incident information is collected using <A.03.06.04E.ODP[02]: 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 | |
| A.03.06.04E.ODP[02] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | automated mechanisms used to collect incident information are defined. | 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 | |
| DS-A.03.06.04E[03] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | incident information is analyzed using <A.03.06.04E.ODP[03]: 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 | |
| A.03.06.04E.ODP[03] | Automated Tracking, Data Collection, and Analysis for Incident Monitoring | automated mechanisms used to analyze incident information are defined. | 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 | |
| 03.07.01E | Software Updates and Patches for Maintenance Tools | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.07.01E | Software Updates and Patches for Maintenance Tools | maintenance tools are inspected to ensure that 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 | |
| 03.08.01E | Dual Authorization for Media Sanitization | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.08.01E | Dual Authorization for Media Sanitization | dual authorization for the sanitization of <A.03.08.01E.ODP[01]: system media> is enforced. | 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 | |
| A.03.08.01E.ODP[01] | Dual Authorization for Media Sanitization | system media to be sanitized using dual authorization is defined. | Functional | Intersects With | System Media Sanitization | DCH-09 | Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | |
| 03.08.02E | Dual Authorization for System Backup Deletion and Destruction | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.08.02E | Dual Authorization for System Backup Deletion and Destruction | dual authorization for the deletion or destruction of <A.03.08.02E.ODP[01]: system backup information> is enforced. | 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 | |
| A.03.08.02E.ODP[01] | Dual Authorization for System Backup Deletion and Destruction | backup information for which to enforce dual authorization in order to delete or destroy is defined. | 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 | |
| 03.08.03E | Testing System Backups for Reliability and Integrity | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.08.03E[01] | Testing System Backups for Reliability and Integrity | backup information is tested <A.03.08.03E.ODP[01]: frequency> to verify media reliability. | 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 | |
| A.03.08.03E.ODP[01] | Testing System Backups for Reliability and Integrity | the frequency at which to test backup information for media reliability is defined. | 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 | |
| DS-A.03.08.03E[02] | Testing System Backups for Reliability and Integrity | backup information is tested <A.03.08.03E.ODP[02]: frequency> to verify 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 | |
| A.03.08.03E.ODP[02] | Testing System Backups for Reliability and Integrity | the frequency at which to test backup information for information integrity is defined. | 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 | |
| 03.08.04E | System Recovery and Reconstitution | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.08.04E[01] | System Recovery and Reconstitution | the recovery of the system to a known state is provided within <A.03.08.04E.ODP[01]: time period> after a disruption, compromise, or failure. | 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 | |
| A.03.08.04E.ODP[01] | System Recovery and Reconstitution | a time period consistent with recovery time and recovery point objectives for the recovery of the system is determined. | 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.08.04E[02] | System Recovery and Reconstitution | the reconstitution of the system to a known state is provided within <A.03.08.04E.ODP[02]: time period> 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 | |
| A.03.08.04E.ODP[02] | System Recovery and Reconstitution | a time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined. | 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 | |
| 03.09.01E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.09.02E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.09.03E | Access Agreements | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.09.03E.a | Access Agreements | access agreements are developed and documented 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 | |
| DS-A.03.09.03E.b[01] | Access Agreements | access agreements are reviewed <A.03.09.03E.ODP[01]: 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 | |
| A.03.09.03E.ODP[01] | Access Agreements | the frequency at which to review and update access agreements is defined. | 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 | |
| DS-A.03.09.03E.b[02] | Access Agreements | access agreements are updated <A.03.09.03E.ODP[01]: 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 | |
| DS-A.03.09.03E.c.01 | Access Agreements | individuals requiring access to CUI and systems processing, storing, or transmitting CUI sign appropriate access agreements prior to being granted access. | 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 | |
| DS-A.03.09.03E.c.02 | Access Agreements | individuals requiring access to CUI and systems processing, storing, or transmitting CUI re-sign access agreements to maintain access when access agreements have been updated or <A.03.09.03E.ODP[02]: 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 | |
| A.03.09.03E.ODP[02] | Access Agreements | the frequency at which to re-sign access agreements to maintain access systems processing, storing, or transmitting CUI is defined. | 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 | |
| 03.09.04E | Citizenship Requirements | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.09.04E | Citizenship Requirements | individuals accessing a system processing, storing, or transmitting CUI meet <A.03.09.04E.ODP[01] 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 citizenship. | 5 | |
| A.03.09.04E.ODP[01] | Citizenship Requirements | Citizenship requirements to be met by individuals to access a system processing, storing, or transmitting CUI are defined. | Functional | Intersects With | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 5 | |
| 03.10.01E | Intrusion Alarms and Surveillance Equipment | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.10.01E[01] | Intrusion Alarms and Surveillance Equipment | physical access to the facility where the system resides is monitored using physical intrusion alarms. | Functional | Intersects With | Monitoring Physical Access To Critical Systems | PES-05.2 | Facility security mechanisms exist to monitor physical access to critical systems or sensitive and/or regulated data, in addition to the physical access monitoring of the facility. | 5 | |
| A.03.10.01E.ODP[01] | Intrusion Alarms and Surveillance Equipment | the time period for which to maintain visitor access records for the facility in which the system resides is defined. | 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 | |
| A.03.10.01E.ODP[01] | Intrusion Alarms and Surveillance Equipment | the time period for which to maintain visitor access records for the facility in which the system resides is defined. | 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 | |
| DS-A.03.10.01E[02] | Intrusion Alarms and Surveillance Equipment | physical access to the facility where the system resides is monitored using physical 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 | |
| DS-A.03.10.01E[02] | Intrusion Alarms and Surveillance Equipment | physical access to the facility where the system resides is monitored using physical 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 | |
| 03.10.02E | Delivery and Removal of System Components | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.10.02E.a[01] | Delivery and Removal of System Components | <A.03.10.02E.ODP[01]: types of system components> are authorized when entering the facility. | 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 | |
| A.03.10.02E.ODP[01] | Delivery and Removal of System Components | the types of system components to be authorized and controlled when entering the facility are defined. | 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 | |
| DS-A.03.10.02E.a[02] | Delivery and Removal of System Components | <A.03.10.02E.ODP[01]: types of system components> are controlled when entering the facility. | 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 | |
| DS-A.03.10.02E.a[03] | Delivery and Removal of System Components | <A.03.10.02E.ODP[02]: types of system components> are authorized when exiting the facility. | 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 | |
| A.03.10.02E.ODP[02] | Delivery and Removal of System Components | the types of system components to be authorized and controlled when exiting the facility are defined. | 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 | |
| DS-A.03.10.02E.a[04] | Delivery and Removal of System Components | <A.03.10.02E.ODP[02]: types of system components> are controlled when exiting the facility. | 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 | |
| DS-A.03.10.02E.b | Delivery and Removal of System Components | records of the system components entering and exiting the facility are maintained. | Functional | Intersects With | Monitoring Physical Access | PES-05 | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents. | 5 | |
| 03.11.01E | Threat Awareness Program | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.01E | Threat Awareness Program | a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence is implemented. | Functional | Intersects With | Threat Intelligence Program | THR-01 | Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities. | 5 | |
| 03.11.02E | Threat Hunting | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.02E.a.01[01] | Threat Hunting | a cyber threat-hunting capability is established to search for indicators of compromise in organizational systems. | Functional | Intersects With | Indicators of Compromise (IOC) | IRO-03 | Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events. | 5 | |
| DS-A.03.11.02E.a.01[01] | Threat Hunting | a cyber threat-hunting capability is established to search for indicators of compromise in organizational systems. | Functional | Intersects With | Monitoring for Indicators of Compromise (IOC) | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC). | 5 | |
| DS-A.03.11.02E.a.01[02] | Threat Hunting | a cyber threat-hunting capability is maintained to search for indicators of compromise in organizational systems. | 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 | |
| DS-A.03.11.02E.a.02[01] | Threat Hunting | a cyber threat-hunting capability is established to detect, track, and disrupt threats that evade existing safeguards. | 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 | |
| DS-A.03.11.02E.a.02[02] | Threat Hunting | a cyber threat-hunting capability is maintained to detect, track, and disrupt threats that evade existing safeguards. | 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 | |
| DS-A.03.11.02E.b | Threat Hunting | the threat-hunting capability is employed<A.03.11.02E.ODP[01]: 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 | |
| A.03.11.02E.ODP[01] | Threat Hunting | the frequency at which to implement the threat-hunting capability is defined. | 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 | |
| 03.11.03E | Predictive Cyber Analytics | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.03E[01] | Predictive Cyber Analytics | <A.03.11.03E.ODP[01]: advanced automation capabilities> are employed to predict and identify risks to <A.03.11.03E.ODP[02]: systems or system components>. | 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 | |
| A.03.11.03E.ODP[01] | Predictive Cyber Analytics | advanced automation capabilities to predict and identify risks are defined. | 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 | |
| A.03.11.03E.ODP[02] | Predictive Cyber Analytics | systems or system components in which advanced automation and analytics capabilities are to be employed are defined. | 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 | |
| DS-A.03.11.03E[02] | Predictive Cyber Analytics | <A.03.11.03E.ODP[03]: advanced analytics capabilities> are employed to predict and identify risks to <A.03.11.03E.ODP[02]: systems or system components>. | 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| A.03.11.03E.ODP[03] | Predictive Cyber Analytics | advanced analytics capabilities to predict and identify risks are defined. | 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 | |
| 03.11.04E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.11.05E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.11.06E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.11.07E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.11.08E | Dynamic Threat Awareness | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.08E | Dynamic Threat Awareness | the current cyber threat environment is determined on an ongoing basis using <A.03.11.08E.ODP[01]: 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 | |
| A.03.11.08E.ODP[01] | Dynamic Threat Awareness | the means to determine the current cyber threat environment on an ongoing basis are defined. | Functional | Intersects With | Dynamic Threat Awareness | THR-01.1 | Mechanisms exist to determine and maintain ongoing awareness of the current cyber threat environment. | 5 | |
| 03.11.09E | Indicators of Compromise | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.09E[01] | Indicators of Compromise | indicators of compromise provided by <A.03.11.09E.ODP[01]: sources> are discovered. | 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 | |
| A.03.11.09E.ODP[01] | Indicators of Compromise | sources that provide indicators of compromise are defined. | 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 | |
| DS-A.03.11.09E[02] | Indicators of Compromise | indicators of compromise provided by <A.03.11.09E.ODP[01]: sources> are collected. | 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 | |
| DS-A.03.11.09E[03] | Indicators of Compromise | indicators of compromise provided by <A.03.11.09E.ODP[01]: sources> are distributed to <A.03.11.09E.ODP[02]: 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 | |
| A.03.11.09E.ODP[02] | Indicators of Compromise | personnel or roles to whom indicators of compromise are to be distributed are defined. | Functional | Intersects With | Incident Response Operations | IRO-01 | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. | 5 | |
| 03.11.10E | Criticality Analysis | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.10E | Criticality Analysis | critical system components and functions are identified by performing a criticality analysis for <A.03.11.10E.ODP[01]: systems, system components, or system services> at <A.03.11.10E.ODP[02]: decision points>. | 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 | |
| DS-A.03.11.10E | Criticality Analysis | critical system components and functions are identified by performing a criticality analysis for <A.03.11.10E.ODP[01]: systems, system components, or system services> at <A.03.11.10E.ODP[02]: decision points>. | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-05 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and | 5 | |
| A.03.11.10E.ODP[01] | Criticality Analysis | systems, system components, or system services to be analyzed for criticality are defined. | 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 | |
| A.03.11.10E.ODP[01] | Criticality Analysis | systems, system components, or system services to be analyzed for criticality are defined. | 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 | |
| A.03.11.10E.ODP[02] | Criticality Analysis | decision points in the system development life cycle when a criticality analysis is to be performed are defined. | 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 | |
| 03.11.11E | Discoverable Information | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.11E[01] | Discoverable Information | discoverable information about the system is identified. | 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 non-compliant Technology Assets, Applications and/or Services (TAAS). | 5 | |
| A.03.11.11E.ODP[01] | Discoverable Information | corrective actions to be taken if information about the system is discoverable are defined. | Functional | Intersects With | Vulnerability Remediation Process | VPM-02 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 5 | |
| DS-A.03.11.11E[02] | Discoverable Information | <A.03.11.11E.ODP[01]: corrective actions> are taken when information about the system is confirmed as discoverable. | Functional | Intersects With | Vulnerability Remediation Process | VPM-02 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 5 | |
| 03.11.12E | Automated Means for Sharing Threat Intelligence | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.11.12E | Automated Means for Sharing Threat Intelligence | automated mechanisms are employed 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 | |
| 03.12.01E | Penetration Testing | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.12.01E | Penetration Testing | penetration testing is conducted <A.03.12.01E.ODP[01]: frequency> on <A.03.12.01E.ODP[02]: 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 | |
| A.03.12.01E.ODP[01] | Penetration Testing | the frequency at which to conduct penetration testing on systems or system components is defined. | 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 | |
| A.03.12.01E.ODP[02] | Penetration Testing | systems or system components on which penetration testing is to be conducted are defined. | Functional | Intersects With | Attack Surface Scope | VPM-01.1 | Mechanisms exist to define and manage the scope for its attack surface management activities. | 5 | |
| 03.12.02E | Independent Assessors | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.12.02E | Independent Assessors | independent assessors or assessment teams are used 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 | |
| 03.12.03E | Risk Monitoring | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.12.03E[01] | Risk Monitoring | risk monitoring is an integral part of the continuous monitoring strategy. | 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, compliance and change management. | 5 | |
| DS-A.03.12.03E[02] | Risk Monitoring | effectiveness monitoring is included in risk 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 | |
| DS-A.03.12.03E[03] | Risk Monitoring | compliance monitoring is included in risk 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 | |
| DS-A.03.12.03E[04] | Risk Monitoring | change monitoring is included in risk 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 | |
| 03.12.04E | Internal System Connections | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.12.04E.a | Internal System Connections | internal connections of <A.03.12.04E.ODP[01]: system components or classes of components> to the system are authorized. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| A.03.12.04E.ODP[01] | Internal System Connections | system components or classes of components requiring internal connections to the system are defined. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| DS-A.03.12.04E.b[01] | Internal System Connections | for each internal connection, the interface characteristics are documented. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.12.04E.b[02] | Internal System Connections | for each internal connection, the security requirements are documented. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| DS-A.03.12.04E.b[03] | Internal System Connections | for each internal connection, the nature of the information communicated is documented. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| DS-A.03.12.04E.c | Internal System Connections | internal system connections are terminated after <A.03.12.04E.ODP[02]: conditions>. | 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 | |
| DS-A.03.12.04E.c | Internal System Connections | internal system connections are terminated after <A.03.12.04E.ODP[02]: conditions>. | 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 | |
| A.03.12.04E.ODP[02] | Internal System Connections | conditions requiring the termination of internal connections are defined. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| DS-A.03.12.04E.d | Internal System Connections | the continued need for each internal connection is reviewed <A.03.12.04E.ODP[03]: frequency>. | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | |
| A.03.12.04E.ODP[03] | Internal System Connections | the frequency at which to review the continued need for each internal connection is defined. | 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 | |
| 03.13.01E | Heterogeneity | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.01E | Heterogeneity | a diverse set of information technologies is employed for <A.03.13.01E.ODP[01]: system components> in the implementation of the system. | 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 | |
| A.03.13.01E.ODP[01] | Heterogeneity | system components requiring a diverse set of information technologies to be used in the implementation of the system are defined. | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-05 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and | 5 | |
| A.03.13.01E.ODP[01] | Heterogeneity | system components requiring a diverse set of information technologies to be used in the implementation of the system are defined. | Functional | Intersects With | Business Process Definition | PRM-06 | Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:<br>(1) The resulting risk to organizational operations, assets, individuals and other organizations; and<br>(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. | 5 | |
| 03.13.02E | Randomness | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.02E | Randomness | <A.03.13.02E.ODP[01]: techniques> are employed 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 | |
| A.03.13.02E.ODP[01] | Randomness | the techniques employed to introduce randomness into organizational operations and assets are defined. | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-05 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and | 5 | |
| 03.13.03E | Concealment and Misdirection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.03E | Concealment and Misdirection | <A.03.13.03E.ODP[01]: concealment and misdirection techniques> are used to mislead adversaries. | 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 | |
| A.03.13.03E.ODP[01] | Concealment and Misdirection | the concealment and misdirection techniques used to confuse and mislead adversaries potentially targeting systems are defined. | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-05 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and | 5 | |
| 03.13.04E | Isolation of System Components | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.04E | Isolation of System Components | boundary protection mechanisms are employed to isolate <A.03.13.04E.ODP[01]: 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 | |
| A.03.13.04E.ODP[01] | Isolation of System Components | system components to be isolated by boundary protection mechanisms are defined. | 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 | |
| 03.13.05E | Change Processing and Storage Locations | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.05E | Change Processing and Storage Locations | the location of <A.03.13.05E.ODP[01]: processing and/or storage> is changed <A.03.13.05E.ODP[02]: SELECTED PARAMETER VALUE>. | 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 | |
| A.03.13.05E.ODP[01] | Change Processing and Storage Locations | processing and/or storage locations to be changed are defined. | 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 | |
| A.03.13.05E.ODP[02] | Change Processing and Storage Locations | one of the following PARAMETER VALUES is selected: {<A.03.13.05E.ODP[03] 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 | |
| A.03.13.05E.ODP[03] | Change Processing and Storage Locations | the frequency at which to change the location of processing and/or storage is defined (if selected). | 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 | |
| 03.13.06E | Platform-Independent Applications | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.06E | Platform-Independent Applications | <A.03.13.06E.ODP[01]: platform-independent applications> are implemented within organizational systems. | Functional | Intersects With | Mobile Code | END-10 | Mechanisms exist to address mobile code / operating system-independent applications. | 5 | |
| A.03.13.06E.ODP[01] | Platform-Independent Applications | platform-independent applications to be included within organizational systems are defined. | 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 | |
| A.03.13.06E.ODP[01] | Platform-Independent Applications | platform-independent applications to be included within organizational systems are defined. | 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 | |
| 03.13.07E | Virtualization Techniques | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.07E | Virtualization Techniques | virtualization techniques are employed to support the deployment of a diverse range of operating systems and applications that are changed <A.03.13.07E.ODP[01]: 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 | |
| A.03.13.07E.ODP[01] | Virtualization Techniques | the frequency at which to change the diversity of operating systems and applications deployed using virtualization techniques is defined. | 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 | |
| 03.13.08E | Decoys | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.08E[01] | Decoys | components within organizational systems specifically designed to be the target of malicious attacks are included to detect 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 | |
| DS-A.03.13.08E[02] | Decoys | components within organizational systems specifically designed to be the target of malicious attacks are included to deflect 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 | |
| DS-A.03.13.08E[03] | Decoys | components within organizational systems specifically designed to be the target of malicious attacks are included to analyze 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 | |
| 03.13.09E | Isolation of Security Tools, Mechanisms, and Support Components | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.13.09E | Isolation of Security Tools, Mechanisms, and Support Components | <A.03.13.09E.ODP[01]: information security tools, mechanisms, and support components> are isolated from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system. | 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 | |
| A.03.13.09E.ODP[01] | Isolation of Security Tools, Mechanisms, and Support Components | information security tools, mechanisms, and support components to be isolated from other internal system components are defined. | 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 | |
| 03.13.10E | Separate Subnetworks | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.10E | Separate Subnetworks | separate network addresses are implemented 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 | |
| 03.13.11E | Thin Nodes | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.11E[01] | Thin Nodes | minimal functionality for <A.03.13.11E.ODP[01]: system components> is employed. | Functional | Intersects With | Thin Nodes | END-11 | Mechanisms exist to configure thin nodes to have minimal functionality and information storage. | 5 | |
| A.03.13.11E.ODP[01] | Thin Nodes | system components to be implemented with minimal functionality and information storage are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| DS-A.03.13.11E[02] | Thin Nodes | minimal information storage on <A.03.13.11E.ODP[01]: system components> is employed. | 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 | |
| 03.13.12E | Denial-of-Service Protection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.12E.a | Denial-of-Service Protection | the effects of <A.03.13.12E.ODP[01]: types of denial-of-service events> are <A.03.13.12E.ODP[02]: SELECTED PARAMETER VALUE>. | 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 | |
| A.03.13.12E.ODP[01] | Denial-of-Service Protection | the types of denial-of-service events to be protected against or limited are defined. | 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 | |
| A.03.13.12E.ODP[02] | Denial-of-Service Protection | one of the following PARAMETER VALUES is selected: {protected against; limited}. | 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 | |
| DS-A.03.13.12E.b | Denial-of-Service Protection | <A.03.13.12E.ODP[03]: safeguards> are employed to protect against or limit the effects 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 | |
| DS-A.03.13.12E.b | Denial-of-Service Protection | <A.03.13.12E.ODP[03]: safeguards> are employed to protect against or limit the effects of denial-of-service events. | 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 | |
| DS-A.03.13.12E.b | Denial-of-Service Protection | <A.03.13.12E.ODP[03]: safeguards> are employed to protect against or limit the effects of denial-of-service events. | 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 | |
| DS-A.03.13.12E.b | Denial-of-Service Protection | <A.03.13.12E.ODP[03]: safeguards> are employed to protect against or limit the effects of denial-of-service events. | 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 | |
| A.03.13.12E.ODP[03] | Denial-of-Service Protection | the safeguards to prevent the denial-of-service objective by type of denial-of-service event are defined. | 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 | |
| 03.13.13E | Port and Input/Output Device Access | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.13E | Port and Input/Output Device Access | <A.03.13.13E.ODP[01]: connection ports or input/output devices> are <A.03.13.13E.ODP[02]: SELECTED PARAMETER VALUE> disabled or removed on <A.03.13.13E.ODP[03]: 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 | |
| A.03.13.13E.ODP[01] | Port and Input/Output Device Access | connection ports or input/output devices to be disabled or removed are defined. | 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 | |
| A.03.13.13E.ODP[02] | Port and Input/Output Device Access | one of the following PARAMETER VALUES is selected: {physically; logically}. | 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 | |
| A.03.13.13E.ODP[03] | Port and Input/Output Device Access | systems or system components with connection ports or input/output devices to be disabled or removed are defined. | 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 | |
| 03.13.14E | Detonation Chambers | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.14E | Detonation Chambers | a detonation chamber capability is employed within the <A.03.13.14E.ODP[01]: 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 | |
| A.03.13.14E.ODP[01] | Detonation Chambers | the system, system component, or location in which a detonation chamber capability is to be employed is defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.13.15E | Separate Subnets to Isolate System Components and Functions | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.15E | Separate Subnets to Isolate System Components and Functions | subnetworks are separated <A.03.13.15E.ODP[01]: SELECTED PARAMETER VALUE> to isolate <A.03.13.15E.ODP[02]: 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 | |
| DS-A.03.13.15E | Separate Subnets to Isolate System Components and Functions | subnetworks are separated <A.03.13.15E.ODP[01]: SELECTED PARAMETER VALUE> to isolate <A.03.13.15E.ODP[02]: 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 | |
| DS-A.03.13.15E | Separate Subnets to Isolate System Components and Functions | subnetworks are separated <A.03.13.15E.ODP[01]: SELECTED PARAMETER VALUE> to isolate <A.03.13.15E.ODP[02]: critical system components and functions>. | 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 | |
| A.03.13.15E.ODP[01] | Separate Subnets to Isolate System Components and Functions | one of the following PARAMETER VALUES is selected: {physically; logically}. | 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 | |
| A.03.13.15E.ODP[02] | Separate Subnets to Isolate System Components and Functions | critical system components and functions to be isolated are defined. | 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 | |
| 03.13.16E | System Partitioning | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.13.16E | System Partitioning | the system is partitioned into <A.03.13.16E.ODP[01]: system components> residing in separate <A.03.13.16E.ODP[02]: SELECTED PARAMETER VALUE> security domains or environments based on <A.03.13.16E.ODP[03]: circumstances>. | Functional | Intersects With | System Partitioning | SEA-03.1 | Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments. | 5 | |
| A.03.13.16E.ODP[01] | System Partitioning | system components to reside in separate physical or logical domains or environments based on circumstances for the physical or logical separation of components are defined. | Functional | Intersects With | System Partitioning | SEA-03.1 | Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments. | 5 | |
| A.03.13.16E.ODP[02] | System Partitioning | one of the following PARAMETER VALUES is selected: {physical; logical}. | Functional | Intersects With | System Partitioning | SEA-03.1 | Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| A.03.13.16E.ODP[03] | System Partitioning | circumstances for the physical or logical separation of components are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.14.01E | Software, Firmware, and Information Integrity | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.01E.a[01] | Software, Firmware, and Information Integrity | integrity verification tools are employed to detect unauthorized changes to <A.03.14.01E.ODP[01]: software>. | 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 | |
| A.03.14.01E.ODP[01] | Software, Firmware, and Information Integrity | software requiring integrity verification tools to be used to detect unauthorized changes is defined. | 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 | |
| DS-A.03.14.01E.a[02] | Software, Firmware, and Information Integrity | integrity verification tools are employed to detect unauthorized changes to <A.03.14.01E.ODP[02]: firmware>. | 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 | |
| A.03.14.01E.ODP[02] | Software, Firmware, and Information Integrity | firmware requiring integrity verification tools to be used to detect unauthorized changes is defined. | 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 | |
| DS-A.03.14.01E.a[03] | Software, Firmware, and Information Integrity | integrity verification tools are employed to detect unauthorized changes to <A.03.14.01E.ODP[03]: information>. | 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 | |
| A.03.14.01E.ODP[03] | Software, Firmware, and Information Integrity | information requiring integrity verification tools to be used to detect unauthorized changes is defined. | 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 | |
| DS-A.03.14.01E.b[01] | Software, Firmware, and Information Integrity | <A.03.14.01E.ODP[04]: actions> are taken when unauthorized changes to software are detected. | 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 | |
| A.03.14.01E.ODP[04] | Software, Firmware, and Information Integrity | actions to be taken when unauthorized changes to software are detected are defined. | 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 | |
| DS-A.03.14.01E.b[02] | Software, Firmware, and Information Integrity | <A.03.14.01E.ODP[05]: actions> are taken when unauthorized changes to firmware are detected. | 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 | |
| A.03.14.01E.ODP[05] | Software, Firmware, and Information Integrity | actions to be taken when unauthorized changes to firmware are detected are defined. | 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 | |
| DS-A.03.14.01E.b[03] | Software, Firmware, and Information Integrity | <A.03.14.01E.ODP[06]: actions> are taken when unauthorized changes to information are detected. | 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 | |
| A.03.14.01E.ODP[06] | Software, Firmware, and Information Integrity | actions to be taken when unauthorized changes to information are detected are defined. | 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 | |
| 03.14.02E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.14.03E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.14.04E | Refresh From Trusted Sources | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.04E | Refresh From Trusted Sources | the software and data used during system component and service refreshes are obtained from <A.03.14.04E.ODP[01]: 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 | |
| A.03.14.04E.ODP[01] | Refresh From Trusted Sources | trusted sources to obtain software and data for system component and service refreshes are defined. | 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 | |
| 03.14.05E | Non-Persistent Information | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.05E.a | Non-Persistent Information | <A.03.14.05E.ODP[01]: SELECTED PARAMETER VALUE> is performed. | Functional | Intersects With | Non-Persistent Information | SEA-08.2 | Mechanisms exist to:<br>(1) Generate or refresh information per an organization-defined frequency; and<br>(2) Delete information when no longer needed. | 5 | |
| A.03.14.05E.ODP[01] | Non-Persistent Information | one of the following PARAMETER VALUES is selected: {refresh <A.03.14.05E.ODP[02] information> <A.03.14.05E.ODP[03] frequency>; generate <A.03.14.05E.ODP[04] information>}. | Functional | Intersects With | Non-Persistent Information | SEA-08.2 | Mechanisms exist to:<br>(1) Generate or refresh information per an organization-defined frequency; and<br>(2) Delete information when no longer needed. | 5 | |
| A.03.14.05E.ODP[02] | Non-Persistent Information | the information to be refreshed is defined (if selected). | 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 | |
| A.03.14.05E.ODP[03] | Non-Persistent Information | the frequency at which to refresh information is defined (if selected). | 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 | |
| A.03.14.05E.ODP[04] | Non-Persistent Information | the information to be generated on demand is defined (if selected). | 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 | |
| DS-A.03.14.05E.b | Non-Persistent Information | information is deleted when no longer needed. | Functional | Intersects With | Non-Persistent Information | SEA-08.2 | Mechanisms exist to:<br>(1) Generate or refresh information per an organization-defined frequency; and<br>(2) Delete information when no longer needed. | 5 | |
| 03.14.06E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.14.07E | N/A | Withdrawn | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 03.14.08E | Integrity Checks | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.08E[01] | Integrity Checks | an integrity check of <A.03.14.08E.ODP[01]: software> is performed <A.03.14.08E.ODP[02]: SELECTED PARAMETER VALUE(S)>. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| A.03.14.08E.ODP[01] | Integrity Checks | software on which an integrity check is to be performed is defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.14.08E.ODP[02] | Integrity Checks | one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[03] transitional states or security-relevant events>; <A.03.14.08E.ODP[04] frequency>}. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| A.03.14.08E.ODP[03] | Integrity Checks | transitional states or security-relevant events requiring integrity checks (on software) are defined (if selected). | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.14.08E.ODP[04] | Integrity Checks | the frequency at which to perform an integrity check (on software) is defined (if selected). | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| DS-A.03.14.08E[02] | Integrity Checks | an integrity check of <A.03.14.08E.ODP[05]: firmware> is performed <A.03.14.08E.ODP[06]: SELECTED PARAMETER VALUE(S)>. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| A.03.14.08E.ODP[05] | Integrity Checks | firmware on which an integrity check is to be performed is defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.14.08E.ODP[06] | Integrity Checks | one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[07] transitional states or security-relevant events>; <A.03.14.08E.ODP[08] frequency>}. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| A.03.14.08E.ODP[07] | Integrity Checks | transitional states or security-relevant events requiring integrity checks (on firmware) are defined (if selected). | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.14.08E.ODP[08] | Integrity Checks | the frequency at which to perform an integrity check (on firmware) is defined (if selected). | 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 | |
| DS-A.03.14.08E[03] | Integrity Checks | an integrity check of <A.03.14.08E.ODP[09]: information> is performed <A.03.14.08E.ODP[10]: SELECTED PARAMETER VALUE(S)>. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| A.03.14.08E.ODP[09] | Integrity Checks | information on which an integrity check is to be performed is defined. | 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 | |
| A.03.14.08E.ODP[10] | Integrity Checks | one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[11] transitional states or security-relevant events>; <A.03.14.08E.ODP[12] frequency>}. | Functional | Intersects With | Integrity Checks | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware. | 5 | |
| A.03.14.08E.ODP[11] | Integrity Checks | transitional states or security-relevant events requiring integrity checks (of information) are defined (if selected). | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.14.08E.ODP[12] | Integrity Checks | the frequency at which to perform an integrity check (of information) is defined (if selected). | 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 | |
| 03.14.09E | Cryptographic Protection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.09E[01] | Cryptographic Protection | cryptographic mechanisms are implemented to detect unauthorized changes to software. | 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 | |
| DS-A.03.14.09E[02] | Cryptographic Protection | cryptographic mechanisms are implemented to detect unauthorized changes to firmware. | 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 | |
| DS-A.03.14.09E[03] | Cryptographic Protection | cryptographic mechanisms are implemented to detect unauthorized changes to 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 | |
| 03.14.10E | Protection of Boot Firmware | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.10E | Protection of Boot Firmware | <A.03.14.10E.ODP[01]: mechanisms> are implemented to protect the integrity of boot firmware in <A.03.14.10E.ODP[02]: system components>. | Functional | Intersects With | Protection of Boot Firmware | END-06.6 | Automated mechanisms exist to protect the integrity of boot firmware in systems. | 5 | |
| A.03.14.10E.ODP[01] | Protection of Boot Firmware | mechanisms to be implemented to protect the integrity of boot firmware in system components are defined. | Functional | Intersects With | Protection of Boot Firmware | END-06.6 | Automated mechanisms exist to protect the integrity of boot firmware in systems. | 5 | |
| A.03.14.10E.ODP[02] | Protection of Boot Firmware | system components requiring mechanisms to protect the integrity of boot firmware are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.14.11E | Integration of Detection and Response | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.11E | Integration of Detection and Response | the detection of <A.03.14.11E.ODP[01]: changes> are incorporated into the organizational incident response capability. | 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 | |
| DS-A.03.14.11E | Integration of Detection and Response | the detection of <A.03.14.11E.ODP[01]: changes> are incorporated into the organizational incident response capability. | Functional | Intersects With | Endpoint Detection & Response (EDR) | END-06.2 | Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents. | 5 | |
| DS-A.03.14.11E | Integration of Detection and Response | the detection of <A.03.14.11E.ODP[01]: changes> are incorporated into the organizational incident response capability. | 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:<br>(1) Endpoints;<br>(2) On-premises networks;<br>(3) Cloud-based networks;<br>(4) Electronic communications;<br>(5) Applications; and<br>(6) Services. | 5 | |
| A.03.14.11E.ODP[01] | Integration of Detection and Response | security-relevant changes to the system are defined. | 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 | |
| 03.14.12E | Information Input Validation | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.12E | Information Input Validation | the validity of the <A.03.14.12E.ODP[01]: information inputs> is checked. | Functional | Intersects With | Input Data Validation | TDA-18 | Mechanisms exist to check the validity of information inputs. | 5 | |
| A.03.14.12E.ODP[01] | Information Input Validation | information inputs to the system requiring validity checks are defined. | Functional | Intersects With | Input Data Validation | TDA-18 | Mechanisms exist to check the validity of information inputs. | 5 | |
| 03.14.13E | Error Handling | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.13E.a | Error Handling | error messages that provide the information necessary for corrective actions are generated without revealing information that could be exploited. | Functional | Intersects With | Error Handling | TDA-19 | Mechanisms exist to handle error conditions by:<br>(1) Identifying potentially security-relevant error conditions;<br>(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and<br>(3) Revealing error messages only to authorized personnel. | 5 | |
| DS-A.03.14.13E.b | Error Handling | error messages are revealed only to <A.03.14.13E.ODP[01]: personnel or roles>. | Functional | Intersects With | Error Handling | TDA-19 | Mechanisms exist to handle error conditions by:<br>(1) Identifying potentially security-relevant error conditions;<br>(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and<br>(3) Revealing error messages only to authorized personnel. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| A.03.14.13E.ODP[01] | Error Handling | personnel or roles to whom error messages are to be revealed are defined. | Functional | Intersects With | Designated Roles To View Error Messages | TDA-19.1 | Mechanisms exist to:<br>(1) Define personnel and/or role(s) authorized to receive security-relevant error messages; and<br>(2) Restrict access to error messages to authorized personnel and/or role(s). | 5 | |
| 03.14.14E | Memory Protection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.14E | Memory Protection | <A.03.14.14E.ODP[01]: safeguards> are implemented to protect the system memory from unauthorized code execution. | Functional | Intersects With | Memory Protection | SEA-10 | Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution. | 5 | |
| A.03.14.14E.ODP[01] | Memory Protection | safeguards to be implemented to protect the system memory from unauthorized code execution are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.14.15E | Non-Persistent System Components and Services | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.15E.a | Non-Persistent System Components and Services | <A.03.14.15E.ODP[01]: non-persistent system components and services> are implemented. | 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 | |
| A.03.14.15E.ODP[01] | Non-Persistent System Components and Services | non-persistent system components and services to be implemented are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| DS-A.03.14.15E.b | Non-Persistent System Components and Services | <A.03.14.15E.ODP[01]: non-persistent system components and services> are initiated from a known state. | 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 | |
| DS-A.03.14.15E.c | Non-Persistent System Components and Services | <A.03.14.15E.ODP[01]: non-persistent system components and services> are terminated <A.03.14.15E.ODP[02]: SELECTED PARAMETER VALUE(S)>. | 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 | |
| A.03.14.15E.ODP[02] | Non-Persistent System Components and Services | one or more of the following PARAMETER VALUES is/are selected: {upon end of session of use; <A.03.14.15E.ODP[03] 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 | |
| A.03.14.15E.ODP[03] | Non-Persistent System Components and Services | the frequency at which to terminate non-persistent components and services that are initiated in a known state is defined (if selected). | 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 | |
| 03.14.16E | Tainting | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.16E | Tainting | data or capabilities are embedded in <A.03.14.16E.ODP[01]: systems or system components> to determine if CUI has been exfiltrated or improperly removed from the organization. | 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 | |
| A.03.14.16E.ODP[01] | Tainting | systems or system components with data or capabilities to be embedded are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.14.17E | System-Generated Alerts | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.17E | System-Generated Alerts | <A.03.14.17E.ODP[01]: personnel or roles> are alerted when system-generated <A.03.14.17E.ODP[02]: indicators of compromise> occur. | 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 | |
| DS-A.03.14.17E | System-Generated Alerts | <A.03.14.17E.ODP[01]: personnel or roles> are alerted when system-generated <A.03.14.17E.ODP[02]: indicators of compromise> occur. | 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 | |
| DS-A.03.14.17E | System-Generated Alerts | <A.03.14.17E.ODP[01]: personnel or roles> are alerted when system-generated <A.03.14.17E.ODP[02]: indicators of compromise> occur. | 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 | |
| A.03.14.17E.ODP[01] | System-Generated Alerts | personnel or roles to be alerted when indications of compromise or potential compromise occur are defined. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| A.03.14.17E.ODP[02] | System-Generated Alerts | compromise indicators are defined. | 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 | |
| 03.14.18E | Automated Organization-Generated Alerts | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.18E | Automated Organization-Generated Alerts | <A.03.14.18E.ODP[01]: personnel or roles> are alerted using <A.03.14.18E.ODP[02]: automated mechanisms> when <A.03.14.18E.ODP[03]: activities> indicate inappropriate or unusual activities with security implications. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| DS-A.03.14.18E | Automated Organization-Generated Alerts | <A.03.14.18E.ODP[01]: personnel or roles> are alerted using <A.03.14.18E.ODP[02]: automated mechanisms> when <A.03.14.18E.ODP[03]: activities> indicate inappropriate or unusual activities with security implications. | 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 | |
| A.03.14.18E.ODP[01] | Automated Organization-Generated Alerts | personnel or roles to be alerted when indications of inappropriate or unusual activity with security implications occur are defined. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| A.03.14.18E.ODP[02] | Automated Organization-Generated Alerts | automated mechanisms used to alert personnel or roles are defined. | 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 | |
| A.03.14.18E.ODP[03] | Automated Organization-Generated Alerts | activities that trigger alerts to personnel or roles are defined. | 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 | |
| 03.14.19E | Wireless Intrusion Detection | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.14.19E[01] | Wireless Intrusion Detection | a wireless intrusion detection system is employed to identify rogue wireless devices. | Functional | Intersects With | Wireless Network Monitoring | MON-01.5 | Mechanisms exist to monitor wireless network segments for:<br>(1) Rogue wireless devices; and<br>(2) Anomalous and/or hostile activities. | 5 | |
| DS-A.03.14.19E[02] | Wireless Intrusion Detection | a wireless intrusion detection system is employed to detect attack attempts on the system. | Functional | Intersects With | Wireless Network Monitoring | MON-01.5 | Mechanisms exist to monitor wireless network segments for:<br>(1) Rogue wireless devices; and<br>(2) Anomalous and/or hostile activities. | 5 | |
| DS-A.03.14.19E[03] | Wireless Intrusion Detection | a wireless intrusion detection system is employed to detect a potential compromise or breach to the system. | Functional | Intersects With | Wireless Network Monitoring | MON-01.5 | Mechanisms exist to monitor wireless network segments for:<br>(1) Rogue wireless devices; and<br>(2) Anomalous and/or hostile activities. | 5 | |
| 03.15.01E | Security Architecture | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.15.01E.a.01 | Security Architecture | a security architecture for the system that describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI is developed. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.15.01E.a.01 | Security Architecture | a security architecture for the system that describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI is developed. | 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:<br>(1) The Open Group Architecture Framework (TOGAF);<br>(2) Sherwood Applied Business Security Architecture (SABSA); and/or<br>(3) An organization-defined reference architecture. | 5 | |
| DS-A.03.15.01E.a.01 | Security Architecture | a security architecture for the system that describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI is developed. | 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 | |
| DS-A.03.15.01E.a.02 | Security Architecture | a security architecture for the system that describes how the security architecture is integrated into and supports the enterprise architecture is developed. | 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:<br>(1) The Open Group Architecture Framework (TOGAF);<br>(2) Sherwood Applied Business Security Architecture (SABSA); and/or<br>(3) An organization-defined reference architecture. | 5 | |
| DS-A.03.15.01E.a.02 | Security Architecture | a security architecture for the system that describes how the security architecture is integrated into and supports the enterprise architecture is developed. | 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 | |
| DS-A.03.15.01E.a.02 | Security Architecture | a security architecture for the system that describes how the security architecture is integrated into and supports the enterprise architecture is developed. | 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 | |
| DS-A.03.15.01E.a.03 | Security Architecture | a security architecture for the system that describes any assumptions about and dependencies on external systems and services is developed. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| DS-A.03.15.01E.b | Security Architecture | the security architecture is reviewed and updated <A.03.15.01E.ODP[01]: frequency> to reflect changes in the enterprise architecture. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.15.01E.ODP[01] | Security Architecture | the frequency for reviewing and updating the security architecture to reflect changes in the enterprise architecture is defined. | 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 | |
| DS-A.03.15.01E.c | Security Architecture | planned security architecture changes are reflected in system security plans, concept of operations, criticality analyses, organizational procedures, procurements, and acquisitions. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.15.02E | Defense In Depth | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.15.02E.a | Defense In Depth | the security architecture for the system is designed using a defense-in-depth approach. | 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 | |
| DS-A.03.15.02E.b | Defense In Depth | <A.03.15.02E.ODP[01]: security requirements> are allocated to <A.03.15.02E.ODP[02]: architectural layers and locations>. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.15.02E.ODP[01] | Defense In Depth | safeguards to be allocated to architectural layers and locations are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.15.02E.ODP[02] | Defense In Depth | architectural layers and locations are defined. | 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 | |
| DS-A.03.15.02E.c | Defense In Depth | the security requirements allocated to the architectural layers and locations are coordinated and mutually reinforcing. | 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 | |
| 03.15.03E | Supplier Diversity | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.15.03E | Supplier Diversity | <A.03.15.03E.ODP[01]: safeguards> that are allocated to <A.03.15.03E.ODP[02]: architectural layers and locations> 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 | |
| A.03.15.03E.ODP[01] | Supplier Diversity | safeguards to be allocated to architectural layers and locations are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.15.03E.ODP[02] | Supplier Diversity | architectural layers and locations are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.16.01E | Specialization | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.16.01E | Specialization | <A.03.16.01E.ODP[01]: SELECTED PARAMETER VALUE(S)> is/are employed to <A.03.16.01E.ODP[02]: systems or system components> supporting mission-essential services or functions to increase the trustworthiness in those systems or components. | 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 | |
| DS-A.03.16.01E | Specialization | <A.03.16.01E.ODP[01]: SELECTED PARAMETER VALUE(S)> is/are employed to <A.03.16.01E.ODP[02]: 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:<br>(1) Improve functionality;<br>(2) Enhance security and resiliency capabilities;<br>(3) Correct security deficiencies; and<br>(4) Conform with applicable statutory, regulatory and/or contractual obligations. | 5 | |
| A.03.16.01E.ODP[01] | Specialization | one or more of the following PARAMETER VALUES is/are selected: {design modification; augmentation; reconfiguration}. | 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:<br>(1) Improve functionality;<br>(2) Enhance security and resiliency capabilities;<br>(3) Correct security deficiencies; and<br>(4) Conform with applicable statutory, regulatory and/or contractual obligations. | 5 | |
| A.03.16.01E.ODP[02] | Specialization | systems or system components supporting mission-essential services or functions are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 03.17.01E | Notification Agreements | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.17.01E | Notification Agreements | agreements and procedures are established with entities involved in the supply chain for the system, system components, or system service for <A.03.17.01E.ODP[01]: SELECTED PARAMETER VALUE(S)>. | 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 | |
| A.03.17.01E.ODP[01] | Notification Agreements | one or more of the following PARAMETER VALUES is/are selected: {notification of supply chain compromises; results of assessments or audits; provision of <A.03.17.01E.ODP[02]: 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 | |
| A.03.17.01E.ODP[02] | Notification Agreements | information for which agreements and procedures are to be established is defined (if selected). | 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 | |
| 03.17.02E | Inspection of Systems or Components | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.17.02E | Inspection of Systems or Components | <A.03.17.02E.ODP[01]: systems or system components> are inspected <A.03.17.02E.ODP[02]: SELECTED PARAMETER VALUE(S)> to detect tampering. | 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 | |
| A.03.17.02E.ODP[01] | Inspection of Systems or Components | systems or system components that require inspection are defined. | 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:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| A.03.17.02E.ODP[02] | Inspection of Systems or Components | one or more of the following PARAMETER VALUES is/are selected: {at random; <A.03.17.02E.ODP[03]: frequency>; upon <A.03.17.02E.ODP[04]: indications of the need for inspection>}. | 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 | |
| A.03.17.02E.ODP[03] | Inspection of Systems or Components | the frequency at which to inspect systems or system components is defined (if selected). | 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 | |
| A.03.17.02E.ODP[04] | Inspection of Systems or Components | indications of the need for an inspection of systems or system components are defined (if selected). | Functional | Intersects With | Physical Tampering Detection | AST-08 | Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC). | 5 | |
| A.03.17.02E.ODP[04] | Inspection of Systems or Components | indications of the need for an inspection of systems or system components are defined (if selected). | 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 | |
| 03.17.03E | Component Authenticity | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.17.03E.a[01] | Component Authenticity | an anti-counterfeit policy is developed and implemented. | 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 | |
| DS-A.03.17.03E.a[02] | Component Authenticity | anti-counterfeit procedures are developed and implemented. | 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 | |
| DS-A.03.17.03E.a[03] | Component Authenticity | the anti-counterfeit policy and procedures include the means to detect counterfeit components entering the system. | 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 | |
| DS-A.03.17.03E.a[04] | Component Authenticity | the anti-counterfeit policy and procedures include the means to prevent counterfeit components from entering the system. | 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 | |
| DS-A.03.17.03E.b | Component Authenticity | counterfeit system components are reported to <A.03.17.03E.ODP[01]: SELECTED PARAMETER VALUE(S)>. | 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 | |
| A.03.17.03E.ODP[01] | Component Authenticity | one or more of the following PARAMETER VALUES is/are selected: {source of counterfeit component; <A.03.17.03E.ODP[02]: external reporting organizations>; <A.03.17.03E.ODP[03]: 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 | |
| A.03.17.03E.ODP[02] | Component Authenticity | external reporting organizations to whom counterfeit system components are to be reported are defined (if selected). | Functional | Intersects With | Incident Handling | IRO-02 | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery. | 5 | |
| A.03.17.03E.ODP[03] | Component Authenticity | personnel or roles to whom counterfeit system components are to be reported are defined (if selected). | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| 03.17.04E | Provenance | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.17.04E[01] | Provenance | valid provenance is documented for <A.03.17.04E.ODP[01]: 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 | |
| A.03.17.04E.ODP[01] | Provenance | systems, system components, and associated CUI that require valid provenance are defined. | 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 | |
| DS-A.03.17.04E[02] | Provenance | valid provenance is monitored for <A.03.17.04E.ODP[01]: 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 | |

**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 - 172A R3 - Assessing Enhanced Security Requirements for Controlled Unclassified Information
**Focal Document URL:** https://csrc.nist.gov/pubs/sp/800/172/a/r3/final
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-172a-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 |
|---|---|---|---|---|---|---|---|---|---|
| DS-A.03.17.04E[03] | Provenance | valid provenance is maintained for <A.03.17.04E.ODP[01]: 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 | |
| 03.17.05E | Supply Chain Integrity – Pedigree | Determine if: | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| DS-A.03.17.05E[01] | Supply Chain Integrity – Pedigree | <A.03.17.05E.ODP[01]: safeguards> are employed to ensure the integrity of the system and 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 | |
| A.03.17.05E.ODP[01] | Supply Chain Integrity – Pedigree | safeguards employed to ensure the integrity of the system and system component are defined. | 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 | |
| DS-A.03.17.05E[02] | Supply Chain Integrity – Pedigree | <A.03.17.05E.ODP[02]: analysis method> is conducted to ensure the integrity of the system and 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 | |
| A.03.17.05E.ODP[02] | Supply Chain Integrity – Pedigree | an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined. | Functional | Intersects With | Physical Tampering Detection | AST-08 | Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC). | 5 | |
| A.03.17.05E.ODP[02] | Supply Chain Integrity – Pedigree | an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined. | 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:<br>(1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and<br>(2) Physical assessments evaluate assets for evidence of unauthorized access and/or modifications. | 5 | |