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

Focal Document: NIST SP 800-172
Focal Document URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-nist-800-172.pdf

FDE #	CMMC L3	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.1e	N/A	Access Control	Employ dual authorization to execute critical or sensitive system and organizational operations.	Functional	Equal	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	10	
3.1.2e	AC.L3-3.1.2E	Access Control	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3	
3.1.2e	AC.L3-3.1.2E	Access Control	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	3	
3.1.2e	AC.L3-3.1.2E	Access Control	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	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.	8	
3.1.2e	AC.L3-3.1.2E	Access Control	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
3.1.3e	AC.L3-3.1.3E	Access Control	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	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/regulated data is stored, transmitted or processed.	3	
3.1.3e	AC.L3-3.1.3E	Access Control	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	3	
3.1.3e	AC.L3-3.1.3E	Access Control	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	8	
3.1.3e	AC.L3-3.1.3E	Access Control	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
3.2.1e	AT.L3-3.2.1E	Awareness Training	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	3	
3.2.1e	AT.L3-3.2.1E	Awareness Training	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
3.2.1e	AT.L3-3.2.1E	Awareness Training	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
3.2.1e	AT.L3-3.2.1E	Awareness Training	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	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.	3	
3.2.2e	AT.L3-3.2.2E	Awareness Training	Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	Functional	Equal	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity and data protection training that reinforce training objectives.	10	
3.2.2e	AT.L3-3.2.2E	Awareness Training	Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
3.4.1e	CM.L3-3.4.1E	Configuration Management	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
3.4.2e	CM.L3-3.4.2E	Configuration Management	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	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.	8	
3.4.2e	CM.L3-3.4.2E	Configuration Management	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	
3.4.2e	CM.L3-3.4.2E	Configuration Management	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	
3.4.2e	CM.L3-3.4.2E	Configuration Management	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	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	
3.4.3e	CM.L3-3.4.3E	Configuration Management	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
3.5.1e	IA.L3-3.5.1E	Identification and Authentication	Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	3	
3.5.1e	IA.L3-3.5.1E	Identification and Authentication	Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	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	
3.5.2e	N/A	Identification and Authentication	Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	3	
3.5.2e	N/A	Identification and Authentication	Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
3.5.2e	N/A	Identification and Authentication	Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	8	
3.5.3e	IA.L3-3.5.3E	Identification and Authentication	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	8	
3.6.1e	IR.L3-3.6.1E	Incident Response	Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].	Functional	Equal	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10	
3.6.2e	IR.L3-3.6.2E	Incident Response	Establish and maintain a cyber incident response team that can be deployed by the organization within [Assignment: organization-defined 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.	8	
3.9.1e	N/A	Personnel Security	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	3	
3.9.1e	N/A	Personnel Security	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	3	

FDE #	CMMC L3	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.9.1e	N/A	Personnel Security	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	
3.9.1e	N/A	Personnel Security	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
3.9.2e	PS.L3-3.9.2E	Personnel Security	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive/regulated data is cleared and regularly trained to handle the information in question.	3	
3.9.2e	PS.L3-3.9.2E	Personnel Security	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
3.9.2e	PS.L3-3.9.2E	Personnel Security	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	3	
3.9.2e	PS.L3-3.9.2E	Personnel Security	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	Functional	Intersects With	Preventative Access Restriction	HRS-07.3	Mechanisms exist to proactively restrict logical and physical access when an individual with access to sensitive/regulated data is under investigation for personnel sanctions that may lead to employment termination.	8	
3.11.1e	RA.L3-3.11.1E	Risk Assessment	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
3.11.1e	RA.L3-3.11.1E	Risk Assessment	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
3.11.1e	RA.L3-3.11.1E	Risk Assessment	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	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	
3.11.1e	RA.L3-3.11.1E	Risk Assessment	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	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.	3	
3.11.2e	RA.L3-3.11.2E	Risk Assessment	Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.	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	
3.11.2e	RA.L3-3.11.2E	Risk Assessment	Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.	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.	8	
3.11.3e	RA.L3-3.11.3E	Risk Assessment	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.	Functional	Intersects With	Security Orchestration, Automation, and Response (SOAR)	OPS-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	5	
3.11.4e	RA.L3-3.11.4E	Risk Assessment	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.	8	
3.11.5e	RA.L3-3.11.5E	Risk Assessment	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	3	
3.11.5e	RA.L3-3.11.5E	Risk Assessment	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	8	
3.11.5e	RA.L3-3.11.5E	Risk Assessment	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	3	
3.11.5e	RA.L3-3.11.5E	Risk Assessment	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
3.11.5e	RA.L3-3.11.5E	Risk Assessment	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	3	
3.11.6e	RA.L3-3.11.6E	Risk Assessment	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	5	
3.11.6e	RA.L3-3.11.6E	Risk Assessment	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	Functional	Subset Of	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
3.11.6e	RA.L3-3.11.6E	Risk Assessment	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	Functional	Subset Of	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
3.11.7e	RA.L3-3.11.7E	Risk Assessment	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency].	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	3	
3.11.7e	RA.L3-3.11.7E	Risk Assessment	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency].	Functional	Subset Of	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
3.12.1e	CA.L3-3.12.1E	Security Assessment	Conduct penetration testing [Assignment: organization-defined frequency], leveraging automated scanning tools and ad hoc tests using subject matter experts.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
3.13.1e	N/A	System and Communications Protection	Create diversity in [Assignment: organization-defined system components] to reduce the extent of malicious code propagation.	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).	8	
3.13.2e	N/A	System and Communications Protection	Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [Assignment: organization-defined changes and frequency of changes by system and system component].	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
3.13.3e	N/A	System and Communications Protection	Employ [Assignment: organization-defined technical and procedural means] to confuse and mislead adversaries.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	8	
3.13.4e	SC.L3-3.13.4E	System and Communications Protection	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	8	
3.13.4e	SC.L3-3.13.4E	System and Communications Protection	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	Functional	Intersects With	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	8	
3.13.4e	SC.L3-3.13.4E	System and Communications Protection	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	8	
3.13.4e	SC.L3-3.13.4E	System and Communications Protection	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
3.13.4e	SC.L3-3.13.4E	System and Communications Protection	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	Functional	Intersects With	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific sensitive/regulated data is isolated from other data when client-specific sensitive/regulated data is processed or stored within multi-client workspaces.	3	

FDE #	CMMC L3	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.13.5e	N/A	System and Communications Protection	Distribute and relocate the following system functions or resources [Assignment: organization-defined frequency]: [Assignment: organization-defined system functions or resources].	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	8	
3.14.1e	SI.L3-3.14.1E	System and Information Integrity	Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	8	
3.14.1e	SI.L3-3.14.1E	System and Information Integrity	Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	Functional	Intersects With	Cryptographic Hash	CRY-13	Mechanisms exist to utilize hash algorithms to generate a hash value that can be used to validate the integrity of data and/or software.	8	
3.14.1e	SI.L3-3.14.1E	System and Information Integrity	Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	Functional	Intersects With	Integrity Mechanisms for Software / Firmware Updates	TDA-01.2	Mechanisms exist to utilize integrity validation mechanisms for security updates.	3	
3.14.2e	N/A	System and Information Integrity	Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
3.14.2e	N/A	System and Information Integrity	Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
3.14.3e	SI.L3-3.14.3E	System and Information Integrity	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	8	
3.14.3e	SI.L3-3.14.3E	System and Information Integrity	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
3.14.3e	SI.L3-3.14.3E	System and Information Integrity	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
3.14.3e	SI.L3-3.14.3E	System and Information Integrity	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive / regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	3	
3.14.4e	N/A	System and Information Integrity	Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].	Functional	Equal	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.	10	
3.14.5e	N/A	System and Information Integrity	Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.	Functional	Intersects With	Data Storage Location Reviews	BCD-02.4	Mechanisms exist to perform periodic security reviews of storage locations that contain sensitive / regulated data.	8	
3.14.5e	N/A	System and Information Integrity	Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	3	
3.14.6e	SI.L3-3.14.6E	System and Information Integrity	Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
3.14.6e	SI.L3-3.14.6E	System and Information Integrity	Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.	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.	8	
3.14.6e	SI.L3-3.14.6E	System and Information Integrity	Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.	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	
3.14.7e	N/A	System and Information Integrity	Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques].	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.	3	