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

Focal Document: CISA Secure Software Development Attestation Form (SSDAF) (2024)
Focal Document URL: https://www.cisa.gov/secure-software-attestation-form
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dhs-cisa-ssdaf-2024.pdf

FDE #	FDE Name (Related EO 14028 Section)	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	4e(i)	The software is developed and built in secure environments. Those environments are secured by the following actions at a minimum:	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
1	4e(i)	The software is developed and built in secure environments. Those environments are secured by the following actions at a minimum:	Functional	Subset Of	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	10	
1	4e(i)	The software is developed and built in secure environments. Those environments are secured by the following actions at a minimum:	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production.	5	
1	4e(i)	The software is developed and built in secure environments. Those environments are secured by the following actions at a minimum:	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production.	3	
1.a	4e(i)(A)	Separating and protecting each environment involved in developing and building software;	Functional	Subset Of	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	10	Example 1: Use multi-factor, risk-based authentication and conditional access for each environment. Example 2: Use network segmentation and access controls to separate the environments from each other and from production environments, and to separate components from each other
1.a	4e(i)(A)	Separating and protecting each environment involved in developing and building software;	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production.	8	Example 1: Use multi-factor, risk-based authentication and conditional access for each environment. Example 2: Use network segmentation and access controls to separate the environments from each other and from production environments, and to separate components from each other
1.b.	4e(i)(B)	Regularly logging monitoring and auditing trust relationships used for authorization and access:	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
1.b.	4e(i)(B)	Regularly logging monitoring and auditing trust relationships used for authorization and access:	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event	5	
1.b.	4e(i)(B)	Regularly logging monitoring and auditing trust relationships used for authorization and access:	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
1.b.i	4e(i)(B)	to any software development and build environments; and	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
1.b.i	4e(i)(B)	to any software development and build environments; and	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
1.b.ii	4e(i)(B)	among components within each environment;	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	
1.b.ii	4e(i)(B)	among components within each environment;	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
1.c	4e(i)(C)	Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	Functional	Equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or(3) Non-console access to critical TAAS that	10	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Subset Of	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.	10	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	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	8	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an	8	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services	5	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that:(1) Is consistent with and supportive of the organization's security	8	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a	5	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	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	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
1.d	4e(i)(D)	Taking consistent and reasonable steps to document as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	3	
1.e	4e(i)(E)	Encrypting sensitive data such as credentials to the extent practicable and based on risk;	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
1.e	4e(i)(E)	Encrypting sensitive data such as credentials to the extent practicable and based on risk;	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an	8	
1.e	4e(i)(E)	Encrypting sensitive data such as credentials to the extent practicable and based on risk;	Functional	Intersects With	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers:(1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and(2) Use the pre-established, secure	8	
1.e	4e(i)(E)	Encrypting sensitive data such as credentials to the extent practicable and based on risk;	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
1.f	4e(i)(F)	Implementing defensive cybersecurity practices including continuous monitoring of operations and alerts and as necessary responding to suspected and confirmed cyber incidents;	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
1.f	4e(i)(F)	Implementing defensive cybersecurity practices including continuous monitoring of operations and alerts and as necessary responding to suspected and confirmed cyber incidents;	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
1.f	4e(i)(F)	Implementing defensive cybersecurity practices including continuous monitoring of operations and alerts and as necessary responding to suspected and confirmed cyber incidents;	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
1.f	4e(i)(F)	Implementing defensive cybersecurity practices including continuous monitoring of operations and alerts and as necessary responding to suspected and confirmed cyber incidents;	Functional	Subset Of	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.	10	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	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	8	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation	8	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	3	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	3	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Supporting Toolchain	TDA-06.4	Automated mechanisms exist to improve the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle.	8	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2)	3	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	3	
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to	5	

FDE #	FDE Name (Related EO 14028 Section)	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2	4e(iii)	The software producer makes a goodfaith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
3	4e(vi)	The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
3	4e(vi)	The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	Functional	Intersects With	Software Release Integrity Verification	TDA-20.1	Mechanisms exist to publish integrity verification information for software releases.	5	
3	4e(vi)	The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	Functional	Intersects With	Software Escrow	TDA-20.3	Mechanisms exist to escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support.	5	
4	4e(iv)	The software producer employed automated tools or comparable processes that check for security vulnerabilities. In addition:	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2)	8	
4	4e(iv)	The software producer employed automated tools or comparable processes that check for security vulnerabilities. In addition:	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
4	4e(iv)	The software producer employed automated tools or comparable processes that check for security vulnerabilities. In addition:	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	3	
4.a	4e(iv)	The software producer operates these processes on an ongoing basis and prior to product version or update releases;	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2)	8	
4.a	4e(iv)	The software producer operates these processes on an ongoing basis and prior to product version or update releases;	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to	8	
4.b	4e(iv)	The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and	Functional	Subset Of	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.	10	
4.b	4e(iv)	The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
4.b	4e(iv)	The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
4.c	4e(iv)	The software producer operates a vulnerability disclosure program and accepts reviews and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.	Functional	Subset Of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the	10	
4.c	4e(iv)	The software producer operates a vulnerability disclosure program and accepts reviews and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	