NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **CMMC 2.0 Level 1 Assessment Objectives (AOs)**
Focal Document URL: https://dowcio.war.gov/CMMC/Resources-Documentation/
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-fed-dod-cmmc-2-level-1-aos.pdf

CMMC 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
AC.L1-B.1.I[a]	N/A	authorized users are identified;	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.I[b]	N/A	processes acting on behalf of authorized users are identified;	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.Ic]	N/A	devices (and other systems) authorized to connect to the system are identified;	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.I[d]	N/A	system access is limited to authorized users;	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.I[e]	N/A	system access is limited to processes acting on behalf of authorized users; and	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.I[f]	N/A	system access is limited to authorized devices (including other systems).	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC.L1-B.1.II[a]	N/A	the types of transactions and functions that authorized users are permitted to execute are defined; and	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
AC.L1-B.1.II[b]	N/A	system access is limited to the defined types of transactions and functions for authorized users.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
AC.L1-B.1.III[a]	N/A	connections to external systems are identified;	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.III[b]	N/A	the use of external systems is identified;	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.III[c]	N/A	connections to external systems are verified;	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.III[d]	N/A	the use of external systems is verified;	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.III[e]	N/A	connections to external systems are controlled/limited; and	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.III[f]	N/A	the use of external systems is controlled/limited.	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
AC.L1-B.1.IV[a]	N/A	individuals authorized to post or process information on publicly accessible systems are identified;	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
AC.L1-B.1.IV[b]	N/A	procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified;	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
AC.L1-B.1.IV[c]	N/A	a review process is in place prior to posting of any content to publicly accessible systems;	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
AC.L1-B.1.IV[d]	N/A	content on publicly accessible systems is reviewed to ensure that it does not include [FCI]; and	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
AC.L1-B.1.IV[e]	N/A	mechanisms are in place to remove and address improper posting of [FCI].	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
IA.L1-B.1.V[a]	N/A	system users are identified;	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
IA.L1-B.1.V[b]	N/A	processes acting on behalf of users are identified; and	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
IA.L1-B.1.V[c]	N/A	devices accessing the system are identified.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
IA.L1-B.1.VI[a]	N/A	the identity of each user is authenticated or verified as a prerequisite to system access;	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
IA.L1-B.1.VI[b]	N/A	the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
IA.L1-B.1.VI[c]	N/A	the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
MP.L1-B.1.VII[a]	N/A	system media containing [FCI] is sanitized or destroyed before disposal; and	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	
MP.L1-B.1.VII[b]	N/A	system media containing [FCI] is sanitized before it is released for reuse.	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	
PE.L1-B.1.VIII[a]	N/A	authorized individuals allowed physical access are identified;	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
PE.L1-B.1.VIII[b]	N/A	physical access to organizational systems is limited to authorized individuals;	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
PE.L1-B.1.VIII[c]	N/A	physical access to equipment is limited to authorized individuals; and	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
PE.L1-B.1.VIII[d]	N/A	physical access to operating environments is limited to authorized individuals.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
PE.L1-B.1.IX[a]	N/A	visitors are escorted;	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).	5	
PE.L1-B.1.IX[b]	N/A	visitor activity is monitored;	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).	5	
PE.L1-B.1.IX[c]	N/A	audit logs of physical access are maintained;	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).	5	
PE.L1-B.1.IX[d]	N/A	physical access devices are identified;	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).	5	
PE.L1-B.1.IX[e]	N/A	physical access devices are controlled; and	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).	5	
PE.L1-B.1.IX[f]	N/A	physical access devices are managed.	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).	5	
SC.L1-B.1.X[a]	N/A	the external system boundary is 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	
SC.L1-B.1.X[b]	N/A	key internal system boundaries 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	
SC.L1-B.1.X[c]	N/A	communications are monitored at the external system boundary;	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC.L1-B.1.X[d]	N/A	communications are monitored at key internal boundaries;	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC.L1-B.1.X[e]	N/A	communications are controlled at the external system boundary;	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC.L1-B.1.X[f]	N/A	communications are controlled at key internal boundaries;	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	

CMMC 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
SC.L1-B.1.X[g]	N/A	communications are protected at the external system boundary; and	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC.L1-B.1.X[h]	N/A	communications are protected at key internal boundaries.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC.L1-B.1.XI[a]	N/A	publicly accessible system components are identified; and	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	
SC.L1-B.1.XI[b]	N/A	subnetworks for publicly accessible system components are physically or logically separated from internal 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	
SI.L1-B.1.XII[a]	N/A	the time within which to identify system flaws is specified;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XII[b]	N/A	system flaws are identified within the specified time frame;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XII[c]	N/A	the time within which to report system flaws is specified;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XII[d]	N/A	system flaws are reported within the specified time frame;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XII[e]	N/A	the time within which to correct system flaws is specified; and	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XII[f]	N/A	system flaws are corrected within the specified time frame.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI.L1-B.1.XIII[a]	N/A	designated locations for malicious code protection are identified; and	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI.L1-B.1.XIII[b]	N/A	protection from malicious code at designated locations is provided.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI.L1-B.1.XIV[a]	N/A	malicious code protection mechanisms are updated when new releases are available.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI.L1-B.1.XV[a]	N/A	the frequency for malicious code scans is defined;	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI.L1-B.1.XV[b]	N/A	malicious code scans are performed with the defined frequency; and	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI.L1-B.1.XV[c]	N/A	real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	