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: CMMC Self-Assessment Guide Level 1
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-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 (optional)	Notes (optional)
AC.L1-B.1.I[a]	N/A	authorized users are identified;	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	Is a list of authorized users maintained that defines their identities and roles [a]?
AC.L1-B.1.I[b]	N/A	processes acting on behalf of authorized users are identified;	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	N/A
AC.L1-B.1.Ic]	N/A	devices (and other systems) authorized to connect to the system are identified;	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	N/A
AC.L1-B.1.I[d]	N/A	system access is limited to authorized users;	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	Are account requests authorized before system access is granted [d,e,f]?
AC.L1-B.1.I[e]	N/A	system access is limited to processes acting on behalf of authorized users; and	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	Are account requests authorized before system access is granted [d,e,f]?
AC.L1-B.1.I[f]	N/A	system access is limited to authorized devices (including other systems).	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	Are account requests authorized before system access is granted [d,e,f]?
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	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	Are access control lists used to limit access to applications and data based on role and/or identity [a]?
AC.L1-B.1.II[b]	N/A	system access is limited to the defined types of transactions and functions for authorized users.	Functional	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	Is access for authorized users restricted to those parts of the system they are explicitly permitted to use, that is, is access denied by default and allowed by exception (e.g., a person who only performs word-
AC.L1-B.1.III[a]	N/A	connections to external systems are identified;	Functional	Subset Of	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.	10	Are all connections to external systems outside of the assessment scope identified [a]?
AC.L1-B.1.III[b]	N/A	the use of external systems is identified;	Functional	Subset Of	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.	10	Are external systems (e.g., systems managed by OSAs, partners, or vendors; personal devices) that are permitted to connect to or make use of organizational systems identified [b]?
AC.L1-B.1.III[c]	N/A	connections to external systems are verified;	Functional	Subset Of	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.	10	Are methods employed to ensure that only authorized connections are being made to external systems (e.g., requiring log-ins or certificates, access from a specific IP address, or access via VPN) [c,e]?
AC.L1-B.1.III[d]	N/A	the use of external systems is verified;	Functional	Subset Of	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.	10	Are methods employed to confirm that only authorized external systems are connecting (e.g., if employees are receiving company email on personal cell phones, is the OSA checking to verify that only
AC.L1-B.1.III[e]	N/A	connections to external systems are controlled/limited; and	Functional	Subset Of	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.	10	Are methods employed to ensure that only authorized connections are being made to external systems (e.g., requiring log-ins or certificates, access from a specific IP address, or access via VPN) [c,e]?
AC.L1-B.1.III[f]	N/A	the use of external systems is controlled/limited.	Functional	Subset Of	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.	10	Is the use of external systems limited, including by policy or physical control [f]?
AC.L1-B.1.IV[a]	N/A	individuals authorized to post or process information on publicly accessible systems are identified;	Functional	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	N/A
AC.L1-B.1.IV[b]	N/A	procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified;	Functional	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	N/A
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	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	Does information on externally facing systems (e.g., publicly accessible) have a documented approval chain for public release [c]?
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	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	N/A
AC.L1-B.1.IV[e]	N/A	mechanisms are in place to remove and address improper posting of [FCI].	Functional	Subset Of	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	N/A
IA.L1-B.1.V[a]	N/A	system users are identified;	Functional	Subset Of	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.	10	Are unique identifiers issued to individual users (e.g., usernames) [a]?
IA.L1-B.1.V[b]	N/A	processes acting on behalf of users are identified; and	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	Are the processes and service accounts that an authorized user initiates identified (e.g., scripts, automatic updates, configuration updates, vulnerability scans) [b]?
IA.L1-B.1.V[c]	N/A	devices accessing the system are identified.	Functional	Subset Of	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.	10	Are unique device identifiers used for devices that access the system identified [c]?
IA.L1-B.1.VI[a]	N/A	the identity of each user is authenticated or verified as a prerequisite to system access;	Functional	Subset Of	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.	10	Are unique authenticators used to verify user identities (e.g., usernames and passwords) [a]?
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	Subset Of	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.	10	An example of a process acting on behalf of users could be a script that logs in as a person or service account [b]. Can the OSA show that it maintains a record of all of those service accounts for use when
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	Subset Of	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.	10	Are device identifiers used in authentication processes (e.g., MAC address, non- anonymous computer name, certificates) [c]?
MP.L1-B.1.VII[a]	N/A	system media containing [FCI] is sanitized or destroyed before disposal; and	Functional	Subset Of	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	10	Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable [a,b]?
MP.L1-B.1.VII[b]	N/A	system media containing [FCI] is sanitized before it is released for reuse.	Functional	Subset Of	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	10	Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable [a,b]?
PE.L1-B.1.VIII[a]	N/A	authorized individuals allowed physical access are identified;	Functional	Subset Of	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	10	Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued [a]?
PE.L1-B.1.VIII[b]	N/A	physical access to organizational systems is limited to authorized individuals;	Functional	Subset Of	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	10	Has the facility/building manager designated building areas as "sensitive" and designed physical security protections (e.g., guards, locks, cameras, card readers) to limit physical access to the area to
PE.L1-B.1.VIII[c]	N/A	physical access to equipment is limited to authorized individuals; and	Functional	Subset Of	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	10	Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals [c]?
PE.L1-B.1.VIII[d]	N/A	physical access to operating environments is limited to authorized individuals.	Functional	Subset Of	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	10	N/A
PE.L1-B.1.IX[a]	N/A	visitors are escorted;	Functional	Subset Of	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	10	Are personnel required to accompany visitors to areas in a facility with physical access to organizational systems [a]?
PE.L1-B.1.IX[b]	N/A	visitor activity is monitored;	Functional	Subset Of	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	10	Are visitors clearly distinguishable from regular personnel [b]? Is visitor activity monitored (e.g., use of cameras or guards, reviews of secure areas upon visitor departure, review of visitor audit logs) [b]?
PE.L1-B.1.IX[c]	N/A	audit logs of physical access are maintained;	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements [c]? Are visitor access records retained for as long as required [c]?
PE.L1-B.1.IX[d]	N/A	physical access devices are identified;	Functional	Subset Of	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	10	Are lists or inventories of physical access devices maintained (e.g., keys, facility badges, key cards) [d]?
PE.L1-B.1.IX[e]	N/A	physical access devices are controlled; and	Functional	Subset Of	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	10	Is access to physical access devices limited (e.g., granted to, and accessible only by, authorized individuals) [e]?
PE.L1-B.1.IX[f]	N/A	physical access devices are managed.	Functional	Subset Of	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	10	Are physical access devices managed (e.g., revoking key card access when necessary, changing locks as needed, maintaining access control devices and systems) [f]?
SC.L1-B.1.X[a]	N/A	the external system boundary is defined;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	What are the external system boundary components that make up the entry and exit points for data flow (e.g., firewalls, gateways, cloud service boundaries), behind which all system components that handle
SC.L1-B.1.X[b]	N/A	key internal system boundaries are defined;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	What are the internal system boundary components that make up the entry and exit points for key internal data flow (e.g., internal firewalls, routers, any devices that can bridge the connection between one
SC.L1-B.1.X[c]	N/A	communications are monitored at the external system boundary;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data flowing in and out of the external and key internal system boundaries monitored (e.g., connections are logged and able to be reviewed, suspicious traffic generates alerts) [c,d]?
SC.L1-B.1.X[d]	N/A	communications are monitored at key internal boundaries;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data flowing in and out of the external and key internal system boundaries monitored (e.g., connections are logged and able to be reviewed, suspicious traffic generates alerts) [c,d]?
SC.L1-B.1.X[e]	N/A	communications are controlled at the external system boundary;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data traversing the external and internal system boundaries controlled such that connections are denied by default and only authorized connections are allowed [e,f]?
SC.L1-B.1.X[f]	N/A	communications are controlled at key internal boundaries;	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data traversing the external and internal system boundaries controlled such that connections are denied by default and only authorized connections are allowed [e,f]?
SC.L1-B.1.X[g]	N/A	communications are protected at the external system boundary; and	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data flowing in and out of the external and key internal system boundaries protected (e.g., applying encryption when required or prudent, tunneling traffic as needed) [g,h]?
SC.L1-B.1.X[h]	N/A	communications are protected at key internal boundaries.	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	Is data flowing in and out of the external and key internal system boundaries protected (e.g., applying encryption when required or prudent, tunneling traffic as needed) [g,h]?
SC.L1-B.1.X[i]	N/A	publicly accessible system components are identified; and	Functional	Subset Of	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.	10	Are any system components reachable by the public (e.g., internet-facing web servers, VPN gateways, publicly accessible cloud services) [a]?
SC.L1-B.1.X[ii]	N/A	subnetworks for publicly accessible system components are physically or logically separated from internal networks.	Functional	Subset Of	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.	10	Are publicly accessible system components on physically or logically separated subnetworks (e.g., isolated subnetworks using separate, dedicated VLAN segments such as DMZs) [b]?
SI.L1-B.1.XII[a]	N/A	the time within which to identify system flaws is specified;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Is the time frame (e.g., a set number of days) within which system flaw identification activities (e.g., vulnerability scans, configuration scans, manual review) must be performed defined and documented [a]?
SI.L1-B.1.XII[b]	N/A	system flaws are identified within the specified time frame;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Are system flaws (e.g., vulnerabilities, misconfigurations) identified in accordance with the specified time frame [b]?
SI.L1-B.1.XII[c]	N/A	the time within which to report system flaws is specified;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	N/A
SI.L1-B.1.XII[d]	N/A	system flaws are reported within the specified time frame;	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	N/A
SI.L1-B.1.XII[e]	N/A	the time within which to correct system flaws is specified; and	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Is the time frame (e.g., a set number of days dependent on the assessed severity of a flaw) within which system flaws must be corrected defined and documented [e]?
SI.L1-B.1.XII[f]	N/A	system flaws are corrected within the specified time frame.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Are system flaws (e.g., applied security patches, made configuration changes, or implemented workarounds or mitigations) corrected within the specified time frame [f]?
SI.L1-B.1.XIII[a]	N/A	designated locations for malicious code protection are identified; and	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	Are system components (e.g., workstations, servers, email gateways, mobile devices) for which malicious code protection must be provided identified and documented [a]?
SI.L1-B.1.XIII[b]	N/A	protection from malicious code at designated locations is provided.	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	N/A
SI.L1-B.1.XIV[a]	N/A	malicious code protection mechanisms are updated when new releases are available.	Functional	Subset Of	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	10	Is there a defined frequency at which malicious code protection mechanisms must be updated (e.g., frequency of automatic updates or manual processes) [a]?
SI.L1-B.1.XV[a]	N/A	the frequency for malicious code scans is defined;	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	N/A
SI.L1-B.1.XV[b]	N/A	malicious code scans are performed with the defined frequency; and	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	N/A
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	Subset Of	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	10	Are files from media (e.g., USB drives, CD-ROM) included in the definition of external sources and are they being scanned [c]?