C3

CMMC Level 2 Controls & Assessment Objectives

Visualized by C3

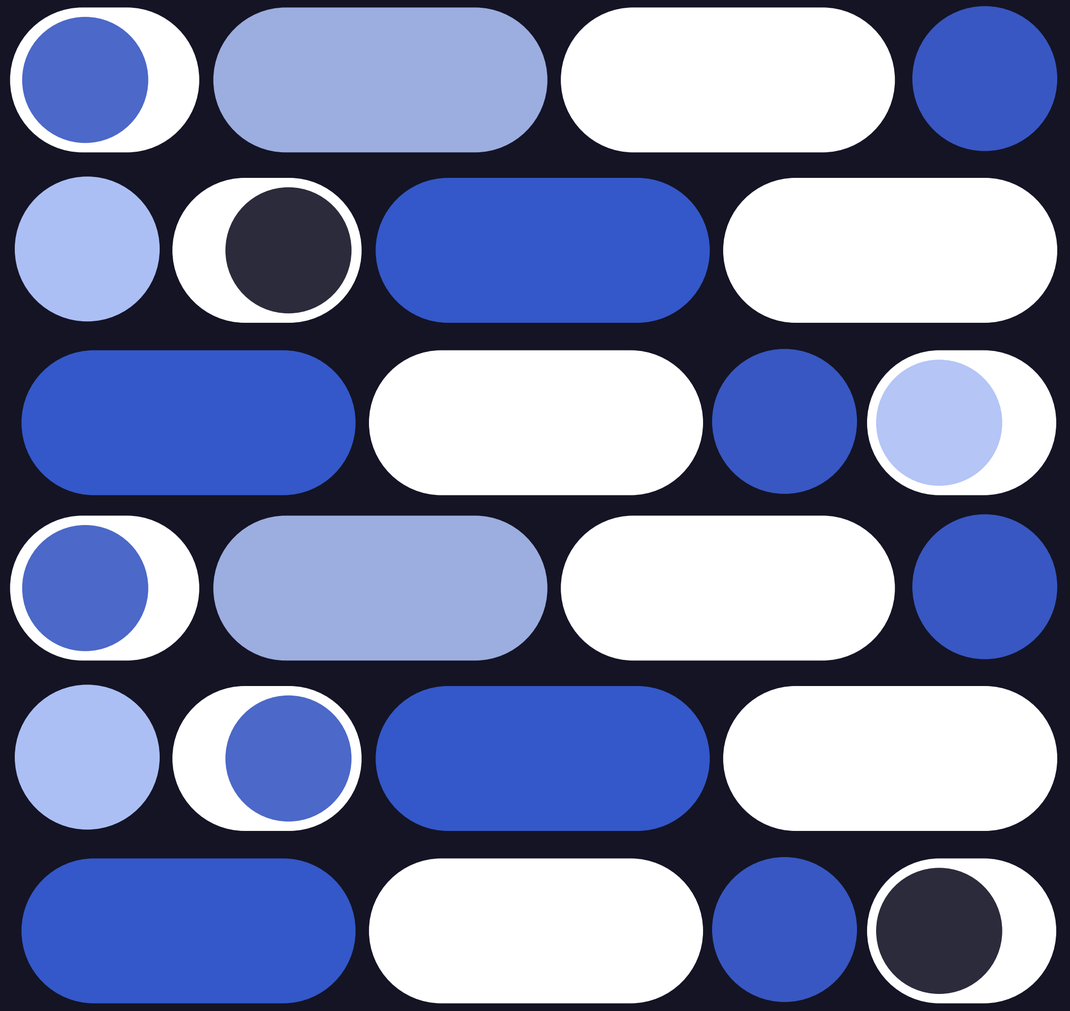
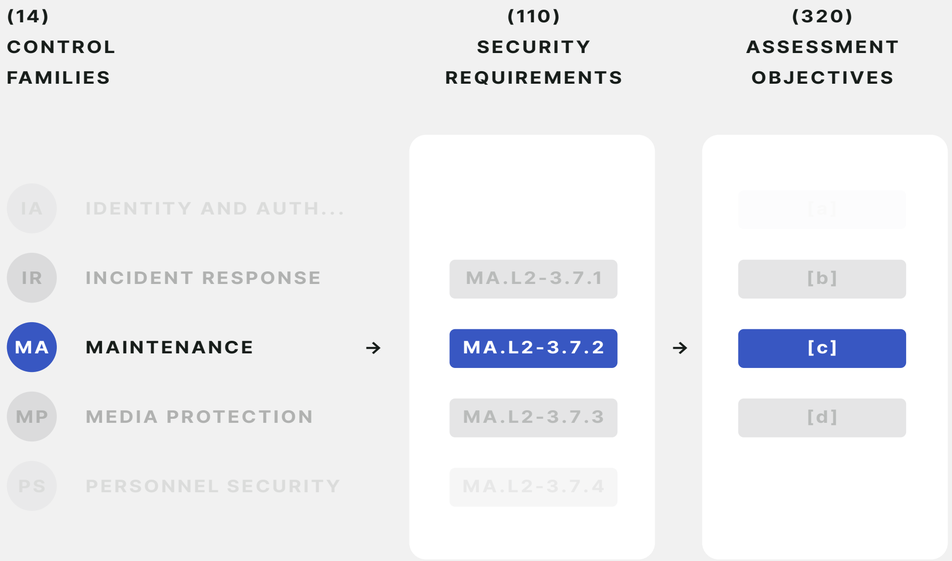


Table of Contents

Introduction



Achieving compliance with CMMC Level 2 is a critical requirement for organizations in the Defense Industrial Base (DIB) that process, store, or transmit Controlled Unclassified Information (CUI). Central to this compliance journey is the implementation of the cybersecurity standards outlined in NIST Special Publication 800-171 Rev. 2. These standards are structured across 14 Security Requirement Families, covering 110 cybersecurity requirements (or controls) designed to protect CUI from unauthorized access.

To ensure that these controls are effectively implemented, NIST Special Publication 800-171A offers an assessment guide that breaks these controls down into 320 detailed assessment objectives. These objectives provide a precise framework for evaluating your organization’s adherence to the necessary cybersecurity protocols and readiness for a CMMC Level 2 assessment.

AC

01

Access Control

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L1-3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	**3.1.1[a]**	Authorized users are identified.
AT	Awareness & Training			**3.1.1[b]**	Processes acting on behalf of authorized users are identified.
AU	Audit & Accountability			**3.1.1[c]**	Devices (and other systems) authorized to connect to the system are identified.
CM	Configuration Management			**3.1.1[d]**	System access is limited to authorized users.
IA	Identification & Authentication			**3.1.1[e]**	System access is limited to processes acting on behalf of authorized users.
IR	Incident Response			**3.1.1[f]**	System access is limited to authorized devices (including other systems).
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L1-3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2[a]	The types of transactions and functions that authorized users are permitted to execute are defined.
AT	Awareness & Training			3.1.2[b]	System access is limited to the defined types of transactions and functions for authorized users.
AU	Audit & Accountability	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[a]	Information flow control policies are defined.
CM	Configuration Management			3.1.3[b]	Methods and enforcement mechanisms for controlling the flow of CUI are defined.
IA	Identification & Authentication			3.1.3[c]	Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
IR	Incident Response			3.1.3[d]	Authorizations for controlling the flow of CUI are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[e]	Approved authorizations for controlling the flow of CUI are enforced.
AT	Awareness & Training	AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	3.1.4[a]	The duties of individuals requiring separation are defined.
AU	Audit & Accountability			3.1.4[b]	Responsibilities for duties that require separation are assigned to separate individuals.
CM	Configuration Management			3.1.4[c]	Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.
IA	Identification & Authentication	AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3.1.5[a]	Privileged accounts are identified.
IR	Incident Response			3.1.5[b]	Access to privileged accounts is authorized in accordance with the principle of least privilege.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3.1.5[c]	Security functions are identified.
AT	Awareness & Training			3.1.5[d]	Access to security functions is authorized in accordance with the principle of least privilege.
AU	Audit & Accountability	AC.L2-3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	3.1.6[a]	Nonsecurity functions are identified.
CM	Configuration Management			3.1.6[b]	Users are required to use non-privileged accounts or roles when accessing nonsecurity functions.
IA	Identification & Authentication	AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	3.1.7[a]	Privileged functions are defined.
IR	Incident Response			3.1.7[b]	Non-privileged users are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	3.1.7[c]	Non-privileged users are prevented from executing privileged functions.
AT	Awareness & Training			3.1.7[d]	The execution of privileged functions is captured in audit logs.
AU	Audit & Accountability	AC.L2-3.1.8	Limit unsuccessful logon attempts.	3.1.8[a]	The means of limiting unsuccessful logon attempts is defined.
CM	Configuration Management			3.1.8[b]	The defined means of limiting unsuccessful logon attempts is implemented.
IA	Identification & Authentication	AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	3.1.9[a]	Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.
IR	Incident Response			3.1.9[b]	Privacy and security notices are displayed.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	**3.1.10[a]**	The period of inactivity after which the system initiates a session lock is defined.
AT	Awareness & Training			**3.1.10[b]**	Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.
AU	Audit & Accountability			**3.1.10[c]**	Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.
CM	Configuration Management	AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.	**3.1.11[a]**	Conditions requiring a user session to terminate are defined.
IA	Identification & Authentication			**3.1.11[b]**	A user session is automatically terminated after any of the defined conditions occur.
IR	Incident Response	AC.L2-3.1.12	Monitor and control remote access sessions.	**3.1.12[a]**	Determine if remote access sessions are permitted.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.12	Monitor and control remote access sessions.	3.1.12[b]	The types of permitted remote access are identified.
AT	Awareness & Training			3.1.12[c]	Remote access sessions are controlled.
AU	Audit & Accountability			3.1.12[d]	Remote access sessions are monitored.
CM	Configuration Management	AC.L2-3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	3.1.13[a]	Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.
IA	Identification & Authentication			3.1.13[b]	Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.
IR	Incident Response	AC.L2-3.1.14	Route remote access via managed access control points.	3.1.14[a]	Managed access control points are identified and implemented.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.14	Route remote access via managed access control points.	3.1.14[b]	Remote access is routed through managed network access control points.
AT	Awareness & Training	AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security- relevant information.	3.1.15[a]	Privileged commands authorized for remote execution are identified.
AU	Audit & Accountability			3.1.15[b]	Security-relevant information authorized to be accessed remotely is identified.
CM	Configuration Management			3.1.15[c]	The execution of the identified privileged commands via remote access is authorized.
IA	Identification & Authentication			3.1.15[d]	Access to the identified security-relevant information via remote access is authorized.
IR	Incident Response	AC.L2-3.1.16	Authorize wireless access prior to allowing such connections.	3.1.16[a]	Wireless access points are identified.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.16	Authorize wireless access prior to allowing such connections.	3.1.16[b]	Wireless access is authorized prior to allowing such connections.
AT	Awareness & Training	AC.L2-3.1.17	Protect wireless access using authentication and encryption.	3.1.17[a]	Wireless access to the system is protected using authentication.
AU	Audit & Accountability			3.1.17[b]	Wireless access to the system is protected using encryption.
CM	Configuration Management	AC.L2-3.1.18	Control connection of mobile devices.	3.1.18[a]	Mobile devices that process, store, or transmit CUI are identified.
IA	Identification & Authentication			3.1.18[b]	Mobile device connections are authorized.
IR	Incident Response			3.1.18[c]	Mobile device connections are monitored and logged.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L2-3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	3.1.19[a]	Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.
AT	Awareness & Training			3.1.19[b]	Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.
AU	Audit & Accountability	AC.L1-3.1.20	Verify and control/limit connections to and use of external systems.	3.1.20[a]	Connections to external systems are identified.
CM	Configuration Management			3.1.20[b]	The use of external systems is identified.
IA	Identification & Authentication			3.1.20[c]	Connections to external systems are verified.
IR	Incident Response			3.1.20[d]	The use of external systems is verified.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AC.L1-3.1.20	Verify and control/limit connections to and use of external systems.	3.1.20[e]	Connections to external systems are controlled/limited.
AT	Awareness & Training			3.1.20[f]	The use of external systems is controlled/limited.
AU	Audit & Accountability	AC.L2-3.1.21	Limit use of portable storage devices on external systems.	3.1.21[a]	The use of portable storage devices containing CUI on external systems is identified and documented.
CM	Configuration Management			3.1.21[b]	Limits on the use of portable storage devices containing CUI on external systems are defined.
IA	Identification & Authentication			3.1.21[c]	The use of portable storage devices containing CUI on external systems is limited as defined.
IR	Incident Response	AC.L1-3.1.22	Control CUI posted or processed on publicly accessible systems.	3.1.22[a]	Individuals authorized to post or process information on publicly accessible systems are identified.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain	
AC	Access Control
AT	Awareness & Training
AU	Audit & Accountability
CM	Configuration Management
IA	Identification & Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PS	Personnel Security
PE	Physical Protection
RA	Risk Assessment
CA	Security Assessment & Authorization
SC	System & Communications Protection
SI	System & Information Integrity

CMMC Practice ID	Security Requirement		Assessment Objective
AC.L1-3.1.22	Control CUI posted or processed on publicly accessible systems.	**3.1.22[b]**	Procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.
		3.1.22[c]	A review process is in place prior to posting of any content to publicly accessible systems.
		3.1.22[d]	Content on publicly accessible systems is reviewed to ensure that it does not include CUI.
		3.1.22[e]	Mechanisms are in place to remove and address improper posting of CUI.

AT

02

Awareness & Training

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AT.L2-3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	3.2.1[a]	Security risks associated with organizational activities involving CUI are identified.
AT	Awareness & Training			3.2.1[b]	Policies, standards, and procedures related to the security of the system are identified.
AU	Audit & Accountability			3.2.1[c]	Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.
CM	Configuration Management			3.2.1[d]	Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization	AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	3.2.2[a]	Information security-related duties, roles, and responsibilities are defined.
SC	System & Communications Protection			3.2.2[b]	Information security-related duties, roles, and responsibilities are assigned to designated personnel.
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	3.2.2[c]	Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.
AT	Awareness & Training	AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	3.2.3[a]	Potential indicators associated with insider threats are identified.
AU	Audit & Accountability			3.2.3[b]	Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

AU

03

Audit & Accountability

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	3.3.1[a]	Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.
AT	Awareness & Training			3.3.1[b]	The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.
AU	Audit & Accountability			3.3.1[c]	Audit records are created (generated).
CM	Configuration Management			3.3.1[d]	Audit records, once created, contain the defined content.
IA	Identification & Authentication			3.3.1[e]	Retention requirements for audit records are defined.
IR	Incident Response			3.3.1[f]	Audit records are retained as defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3.3.2[a]	The content of the audit records needed to support the ability to uniquely trace users to their actions is defined.
AT	Awareness & Training			3.3.2[b]	Audit records, once created, contain the defined content.
AU	Audit & Accountability	AU.L2-3.3.3	Review and update logged events.	3.3.3[a]	A process for determining when to review logged events is defined.
CM	Configuration Management			3.3.3[b]	Event types being logged are reviewed in accordance with the defined review process.
IA	Identification & Authentication			3.3.3[c]	Event types being logged are updated based on the review.
IR	Incident Response	AU.L2-3.3.4	Alert in the event of an audit logging process failure.	3.3.4[a]	Personnel or roles to be alerted in the event of an audit logging process failure are identified.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AU.L2-3.3.4	Alert in the event of an audit logging process failure.	3.3.4[b]	Types of audit logging process failures for which alert will be generated are defined.
AT	Awareness & Training			3.3.4[c]	Identified personnel or roles are alerted in the event of an audit logging process failure.
AU	Audit & Accountability	AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	3.3.5[a]	Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.
CM	Configuration Management			3.3.5[b]	Defined audit record review, analysis, and reporting processes are correlated.
IA	Identification & Authentication	AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	3.3.6[a]	An audit record reduction capability that supports on-demand analysis is provided.
IR	Incident Response			3.3.6[b]	A report generation capability that supports on-demand reporting is provided.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	3.3.7[a]	Internal system clocks are used to generate time stamps for audit records.
AT	Awareness & Training			3.3.7[b]	An authoritative source with which to compare and synchronize internal system clocks is specified.
AU	Audit & Accountability			3.3.7[c]	Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.
CM	Configuration Management	AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	3.3.8[a]	Audit information is protected from unauthorized access.
IA	Identification & Authentication			3.3.8[b]	Audit information is protected from unauthorized modification.
IR	Incident Response			3.3.8[c]	Audit information is protected from unauthorized deletion.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	3.3.8[d]	Audit logging tools are protected from unauthorized access.
AT	Awareness & Training			3.3.8[e]	Audit logging tools are protected from unauthorized modification.
AU	Audit & Accountability			3.3.8[f]	Audit logging tools are protected from unauthorized deletion.
CM	Configuration Management	AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users.	3.3.9[a]	A subset of privileged users granted access to manage audit logging functionality is defined.
IA	Identification & Authentication			3.3.9[b]	Management of audit logging functionality is limited to the defined subset of privileged users.
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

CM

04

Configuration Management

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	3.4.1[a]	A baseline configuration is established.
AT	Awareness & Training			3.4.1[b]	The baseline configuration includes hardware, software, firmware, and documentation.
AU	Audit & Accountability			3.4.1[c]	The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.
CM	Configuration Management			3.4.1[d]	A system inventory is established.
IA	Identification & Authentication			3.4.1[e]	The system inventory includes hardware, software, firmware, and documentation.
IR	Incident Response			3.4.1[f]	The inventory is maintained (reviewed and updated) throughout the system development life cycle.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain

- AC Access Control
- AT Awareness & Training
- AU Audit & Accountability
- CM Configuration Management
- IA Identification & Authentication
- IR Incident Response
- MA Maintenance
- MP Media Protection
- PS Personnel Security
- PE Physical Protection
- RA Risk Assessment
- CA Security Assessment & Authorization
- SC System & Communications Protection
- SI System & Information Integrity

CMMC Practice ID	Security Requirement		Assessment Objective
CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	3.4.2[a]	Security configuration settings for information technology products employed in the system are established and included in the baseline configuration.
		3.4.2[b]	Security configuration settings for information technology products employed in the system are enforced.
CM.L2-3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	3.4.3[a]	Changes to the system are tracked.
		3.4.3[b]	Changes to the system are reviewed.
		3.4.3[c]	Changes to the system are approved or disapproved.
		3.4.3[d]	Changes to the system are logged.

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.	3.4.4[a]	The security impact of changes to the system is analyzed prior to implementation.
AT	Awareness & Training	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	3.4.5[a]	Physical access restrictions associated with changes to the system are defined.
AU	Audit & Accountability			3.4.5[b]	Physical access restrictions associated with changes to the system are documented.
CM	Configuration Management			3.4.5[c]	Physical access restrictions associated with changes to the system are approved.
IA	Identification & Authentication			3.4.5[d]	Physical access restrictions associated with changes to the system are enforced.
IR	Incident Response			3.4.5[e]	Logical access restrictions associated with changes to the system are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	3.4.5[f]	Logical access restrictions associated with changes to the system are documented.
AT	Awareness & Training			3.4.5[g]	Logical access restrictions associated with changes to the system are approved.
AU	Audit & Accountability			3.4.5[h]	Logical access restrictions associated with changes to the system are enforced.
CM	Configuration Management	CM.L2-3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	3.4.6[a]	Essential system capabilities are defined based on the principle of least functionality.
IA	Identification & Authentication			3.4.6[b]	The system is configured to provide only the defined essential capabilities.
IR	Incident Response	CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.4.7[a]	Essential programs are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.4.7[b]	The use of nonessential programs is defined.
AT	Awareness & Training			3.4.7[c]	The use of nonessential programs is restricted, disabled, or prevented as defined.
AU	Audit & Accountability			3.4.7[d]	Essential functions are defined.
CM	Configuration Management			3.4.7[e]	The use of nonessential functions is defined.
IA	Identification & Authentication			3.4.7[f]	The use of nonessential functions is restricted, disabled, or prevented as defined.
IR	Incident Response			3.4.7[g]	Essential ports are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.4.7[h]	The use of nonessential ports is defined.
AT	Awareness & Training			3.4.7[i]	The use of nonessential ports is restricted, disabled, or prevented as defined.
AU	Audit & Accountability			3.4.7[j]	Essential protocols are defined.
CM	Configuration Management			3.4.7[k]	The use of nonessential protocols is defined.
IA	Identification & Authentication			3.4.7[l]	The use of nonessential protocols is restricted, disabled, or prevented as defined.
IR	Incident Response			3.4.7[m]	Essential services are defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.4.7[n]	The use of nonessential services is defined.
AT	Awareness & Training			3.4.7[o]	The use of nonessential services is restricted, disabled, or prevented as defined.
AU	Audit & Accountability	CM.L2-3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	3.4.8[a]	A policy specifying whether whitelisting or blacklisting is to be implemented is specified.
CM	Configuration Management			3.4.8[b]	The software allowed to execute under whitelisting or denied use under blacklisting is specified.
IA	Identification & Authentication			3.4.8[c]	Whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.
IR	Incident Response	CM.L2-3.4.9	Control and monitor user-installed software.	3.4.9[a]	A policy for controlling the installation of software by users is established.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CM.L2-3.4.9	Control and monitor user-installed software.	3.4.9[b]	Installation of software by users is controlled based on the established policy.
AT	Awareness & Training			3.4.9[c]	Installation of software by users is monitored.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

IA

05

Identification & Authentication

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	IA.L2-3.5.1	Identify system users, processes acting on behalf of users, and devices.	3.5.1[a]	System users are identified.
AT	Awareness & Training			3.5.1[b]	Processes acting on behalf of users are identified.
AU	Audit & Accountability			3.5.1[c]	Devices accessing the system are identified.
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection	IA.L2-3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	3.5.2[a]	The identity of each user is authenticated or verified as a prerequisite to system access.
PS	Personnel Security			3.5.2[b]	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.
PE	Physical Protection			3.5.2[c]	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	IA.L2-3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	3.5.3[a]	Privileged accounts are identified.
AT	Awareness & Training			3.5.3[b]	Multifactor authentication is implemented for local access to privileged accounts.
AU	Audit & Accountability			3.5.3[c]	Multifactor authentication is implemented for network access to privileged accounts.
CM	Configuration Management			3.5.3[d]	Multifactor authentication is implemented for network access to non-privileged accounts.
IA	Identification & Authentication	IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	3.5.4[a]	Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.
IR	Incident Response	IA.L2-3.5.5	Prevent reuse of identifiers for a defined period.	3.5.5[a]	A period within which identifiers cannot be reused is defined.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	IA.L2-3.5.5	Prevent reuse of identifiers for a defined period.	3.5.5[b]	Reuse of identifiers is prevented within the defined period.
AT	Awareness & Training	IA.L2-3.5.6	Disable identifiers after a defined period of inactivity.	3.5.6[a]	A period of inactivity after which an identifier is disabled is defined.
AU	Audit & Accountability			3.5.6[b]	Identifiers are disabled after the defined period of inactivity.
CM	Configuration Management	IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	3.5.7[a]	Password complexity requirements are defined.
IA	Identification & Authentication			3.5.7[b]	Password change of character requirements are defined.
IR	Incident Response			3.5.7[c]	Minimum password complexity requirements as defined are enforced when new passwords are created.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	3.5.7[d]	Minimum password change of character requirements as defined are enforced when new passwords are created.
AT	Awareness & Training	IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.	3.5.8[a]	The number of generations during which a password cannot be reused is specified.
AU	Audit & Accountability			3.5.8[b]	Reuse of passwords is prohibited during the specified number of generations.
CM	Configuration Management	IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	3.5.9[a]	Immediate change to a permanent password is required when a temporary password is used for system logon.
IA	Identification & Authentication	IA.L2-3.5.10	Store and transmit only cryptographically- protected passwords.	3.5.10[a]	Passwords are cryptographically protected in storage.
IR	Incident Response			3.5.10[b]	Passwords are cryptographically protected in transit.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain	
AC	Access Control
AT	Awareness & Training
AU	Audit & Accountability
CM	Configuration Management
IA	Identification & Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PS	Personnel Security
PE	Physical Protection
RA	Risk Assessment
CA	Security Assessment & Authorization
SC	System & Communications Protection
SI	System & Information Integrity

CMMC Practice ID	Security Requirement		Assessment Objective
IA.L2-3.5.11	Obscure feedback of authentication information.	3.5.11[a]	Authentication information is obscured during the authentication process.

IR

06

Incident Response

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	3.6.1[a]	An operational incident-handling capability is established.
AT	Awareness & Training			3.6.1[b]	The operational incident-handling capability includes preparation.
AU	Audit & Accountability			3.6.1[c]	The operational incident-handling capability includes detection.
CM	Configuration Management			3.6.1[d]	The operational incident-handling capability includes analysis.
IA	Identification & Authentication			3.6.1[e]	The operational incident-handling capability includes containment.
IR	Incident Response			3.6.1[f]	The operational incident-handling capability includes recovery.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	3.6.1[g]	The operational incident-handling capability includes user response activities.
AT	Awareness & Training	IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	3.6.2[a]	Incidents are tracked.
AU	Audit & Accountability			3.6.2[b]	Incidents are documented.
CM	Configuration Management			3.6.2[c]	Authorities to whom incidents are to be reported are identified.
IA	Identification & Authentication			3.6.2[d]	Organizational officials to whom incidents are to be reported are identified.
IR	Incident Response			3.6.2[e]	Identified authorities are notified of incidents.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain	CMMC Practice ID	Security Requirement		Assessment Objective
IR	IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	3.6.2[f]	Identified organizational officials are notified of incidents.
	IR.L2-3.6.3	Test the organizational incident response capability.	3.6.3[a]	The incident response capability is tested.

MA

07 Maintenance

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	MA.L2-3.7.1	Perform maintenance on organizational systems.	3.7.1[a]	System maintenance is performed.
AT	Awareness & Training	MA.L2-3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	3.7.2[a]	Tools used to conduct system maintenance are controlled.
AU	Audit & Accountability			3.7.2[b]	Techniques used to conduct system maintenance are controlled.
CM	Configuration Management			3.7.2[c]	Mechanisms used to conduct system maintenance are controlled.
IA	Identification & Authentication			3.7.2[d]	Personnel used to conduct system maintenance are controlled.
IR	Incident Response	MA.L2-3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	3.7.3[a]	Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	MA.L2-3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3.7.4[a]	Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.
AT	Awareness & Training	MA.L2-3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	3.7.5[a]	Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.
AU	Audit & Accountability			3.7.5[b]	Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.
CM	Configuration Management	MA.L2-3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	3.7.6[a]	Maintenance personnel without required access authorization are supervised during maintenance activities.
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

MP

08

Media Protection

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	MP.L2-3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3.8.1[a]	Paper media containing CUI is physically controlled.
AT	Awareness & Training			3.8.1[b]	Digital media containing CUI is physically controlled.
AU	Audit & Accountability			3.8.1[c]	Paper media containing CUI is securely stored.
CM	Configuration Management			3.8.1[d]	Digital media containing CUI is securely stored.
IA	Identification & Authentication	MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	3.8.2[a]	Access to CUI on system media is limited to authorized users.
IR	Incident Response	MP.L2-3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	3.8.3[a]	System media containing CUI is sanitized or destroyed before disposal.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	MP.L2-3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	3.8.3[b]	System media containing CUI is sanitized before it is released for reuse.
AT	Awareness & Training	MP.L2-3.8.4	Mark media with necessary CUI markings and distribution limitations.	3.8.4[a]	Media containing CUI is marked with applicable CUI markings.
AU	Audit & Accountability			3.8.4[b]	Media containing CUI is marked with distribution limitations.
CM	Configuration Management	MP.L2-3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	3.8.5[a]	Access to media containing CUI is controlled.
IA	Identification & Authentication			3.8.5[b]	Accountability for media containing CUI is maintained during transport outside of controlled areas.
IR	Incident Response	MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	3.8.6[a]	Confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	MP.L2-3.8.7	Control the use of removable media on system components.	3.8.7[a]	Use of removable media on system components is controlled.
AT	Awareness & Training	MP.L2-3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3.8.8[a]	Use of portable storage devices is prohibited when such devices have no identifiable owner.
AU	Audit & Accountability	MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.	3.8.9[a]	Confidentiality of backup CUI is protected at storage locations.
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

PS

09

Personnel Security

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	PS.L2-3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3.9.1[a]	Individuals are screened prior to authorizing access to organizational systems containing CUI.
AT	Awareness & Training	PS.L2-3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	3.9.2[a]	A policy and/or process for terminating system access and any credentials coincident with personnel actions is established.
AU	Audit & Accountability			3.9.2[b]	System access and credentials are terminated consistent with personnel actions such as termination or transfer.
CM	Configuration Management			3.9.2[c]	The system is protected during and after personnel transfer actions.
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

PE

10

Physical & Environmental Protection

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	PE.L1-3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	3.10.1[a]	Authorized individuals allowed physical access are identified.
AT	Awareness & Training			3.10.1[b]	Physical access to organizational systems is limited to authorized individuals.
AU	Audit & Accountability			3.10.1[c]	Physical access to equipment is limited to authorized individuals.
CM	Configuration Management			3.10.1[d]	Physical access to operating environments is limited to authorized individuals.
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection	PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	3.10.2[a]	The physical facility where organizational systems reside is protected.
RA	Risk Assessment			3.10.2[b]	The support infrastructure for organizational systems is protected.
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	3.10.2[c]	The physical facility where organizational systems reside is monitored.
AT	Awareness & Training			3.10.2[d]	The support infrastructure for organizational systems is monitored.
AU	Audit & Accountability	PE.L2-3.10.3	Escort visitors and monitor visitor activity.	3.10.3[a]	Visitors are escorted.
CM	Configuration Management			3.10.3[b]	Visitor activity is monitored.
IA	Identification & Authentication	PE.L2-3.10.4	Maintain audit logs of physical access.	3.10.4[a]	Audit logs of physical access are maintained.
IR	Incident Response	PE.L2-3.10.5	Control and manage physical access devices.	3.10.5[a]	Physical access devices are identified.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	PE.L2-3.10.5	Control and manage physical access devices.	3.10.5[b]	Physical access devices are controlled.
AT	Awareness & Training			3.10.5[c]	Physical access devices are managed.
AU	Audit & Accountability	PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	3.10.6[a]	Safeguarding measures for CUI are defined for alternate work sites.
CM	Configuration Management			3.10.6[b]	Safeguarding measures for CUI are enforced for alternate work sites.
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

RA

11 Risk Assessment

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	3.11.1[a]	The frequency to assess risk to organizational operations, organizational assets, and individuals is defined.
AT	Awareness & Training			3.11.1[b]	Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	3.11.2[a]	The frequency to scan for vulnerabilities in organizational systems and applications is defined.
MA	Maintenance			3.11.2[b]	Vulnerability scans are performed on organizational systems with the defined frequency.
MP	Media Protection			3.11.2[c]	Vulnerability scans are performed on applications with the defined frequency.
PS	Personnel Security			3.11.2[d]	Vulnerability scans are performed on organizational systems when new vulnerabilities are identified.
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	3.11.2[e]	Vulnerability scans are performed on applications when new vulnerabilities are identified.
AT	Awareness & Training				
AU	Audit & Accountability	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	3.11.3[a]	Vulnerabilities are identified.
CM	Configuration Management				
IA	Identification & Authentication	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	3.11.3[b]	Vulnerabilities are remediated in accordance with risk assessments.
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

CA

12

Security Assessment & Authorization

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CA.L2-3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	3.12.1[a]	The frequency of security control assessments is defined.
AT	Awareness & Training			3.12.1[b]	Security controls are assessed with the defined frequency to determine if the controls are effective in their application.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response	CA.L2-3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3.12.2[a]	Deficiencies and vulnerabilities to be addressed by the plan of action are identified.
MA	Maintenance			3.12.2[b]	A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.
MP	Media Protection			3.12.2[c]	The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection	CA.L2-3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	3.12.3[a]	Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	3.12.4[a]	A system security plan is developed.
AT	Awareness & Training			3.12.4[b]	The system boundary is described and documented in the system security plan.
AU	Audit & Accountability			3.12.4[c]	The system environment of operation is described and documented in the system security plan.
CM	Configuration Management			3.12.4[d]	The security requirements identified and approved by the designated authority as non-applicable are identified.
IA	Identification & Authentication			3.12.4[e]	The method of security requirement implementation is described and documented in the system security plan.
IR	Incident Response			3.12.4[f]	The relationship with or connection to other systems is described and documented in the system security plan.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	3.12.4[g]	The frequency to update the system security plan is defined.
AT	Awareness & Training			3.12.4[h]	System security plan is updated with the defined frequency.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

SC

13

System & Communications Protection

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	SC.L2-3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	3.13.1[a]	The external system boundary is defined.
AT	Awareness & Training			3.13.1[b]	Key internal system boundaries are defined.
AU	Audit & Accountability			3.13.1[c]	Communications are monitored at the external system boundary.
CM	Configuration Management			3.13.1[d]	Communications are monitored at key internal boundaries.
IA	Identification & Authentication			3.13.1[e]	Communications are controlled at the external system boundary.
IR	Incident Response			3.13.1[f]	Communications are controlled at key internal boundaries.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	3.13.1[g]	Communications are protected at the external system boundary.
AT	Awareness & Training			3.13.1[h]	Communications are protected at key internal boundaries.
AU	Audit & Accountability	SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	3.13.2[a]	Architectural designs that promote effective information security are identified.
CM	Configuration Management			3.13.2[b]	Software development techniques that promote effective information security are identified.
IA	Identification & Authentication			3.13.2[c]	Systems engineering principles that promote effective information security are identified.
IR	Incident Response			3.13.2[d]	Identified architectural designs that promote effective information security are employed.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	3.13.2[e]	Identified software development techniques that promote effective information security are employed.
AT	Awareness & Training			3.13.2[f]	Identified systems engineering principles that promote effective information security are employed.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response	SC.L2-3.13.3	Separate user functionality from system management functionality.	3.13.3[a]	User functionality is identified.
MA	Maintenance			3.13.3[b]	System management functionality is identified.
MP	Media Protection			3.13.3[c]	User functionality is separated from system management functionality.
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection	SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	3.13.4[a]	Unauthorized and unintended information transfer via shared system resources is prevented
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5[a]	Publicly accessible system components are identified.
AT	Awareness & Training			3.13.5[b]	Subnetworks for publicly accessible system components are physically or logically separated from internal networks.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response	SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	3.13.6[a]	Network communications traffic is denied by default.
MA	Maintenance			3.13.6[b]	Network communications traffic is allowed by exception.
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment	SC.L2-3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	3.13.7[a]	Remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).
CA	Security Assessment & Authorization				
SC	System & Communications Protection	SC.L2-3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3.13.8[a]	Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3.13.8[b]	Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.
AT	Awareness & Training			3.13.8[c]	Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.
AU	Audit & Accountability	SC.L2-3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	3.13.9[a]	A period of inactivity to terminate network connections associated with communications sessions is defined.
CM	Configuration Management			3.13.9[b]	Network connections associated with communications sessions are terminated at the end of the sessions.
IA	Identification & Authentication			3.13.9[c]	Network connections associated with communications sessions are terminated after the defined period of inactivity.
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	**3.13.10[a]**	Cryptographic keys are established whenever cryptography is employed.
AT	Awareness & Training			**3.13.10[b]**	Cryptographic keys are managed whenever cryptography is employed.
AU	Audit & Accountability	SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	**3.13.11[a]**	FIPS-validated cryptography is employed to protect the confidentiality of CUI.
CM	Configuration Management	SC.L2-3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	**3.13.12[a]**	Collaborative computing devices are identified.
IA	Identification & Authentication			**3.13.12[b]**	Collaborative computing devices provide indication to users of devices in use.
IR	Incident Response			**3.13.12[c]**	Remote activation of collaborative computing devices is prohibited.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SC.L2-3.13.13	Control and monitor the use of mobile code.	3.13.13[a]	Use of mobile code is controlled.
AT	Awareness & Training			3.13.13[b]	Use of mobile code is monitored.
AU	Audit & Accountability	SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	3.13.14[a]	Use of Voice over Internet Protocol (VoIP) technologies is controlled.
CM	Configuration Management			3.13.14[b]	Use of Voice over Internet Protocol (VoIP) technologies is monitored.
IA	Identification & Authentication	SC.L2-3.13.15	Protect the authenticity of communications sessions.	3.13.15[a]	Authenticity of communications sessions is protected.
IR	Incident Response	SC.L2-3.13.16	Protect the confidentiality of CUI at rest.	3.13.16[a]	Confidentiality of CUI at rest is protected.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

SI

14 System & Information Integrity

Domain		CMMC Practice ID	Security Requirement	Assessment Objective	
AC	Access Control	SI.L2-3.14.1	Identify, report, and correct system flaws in a timely manner.	**3.14.1[a]**	The time within which to identify system flaws is specified.
AT	Awareness & Training			**3.14.1[b]**	System flaws are identified within the specified time frame.
AU	Audit & Accountability			**3.14.1[c]**	The time within which to report system flaws is specified.
CM	Configuration Management			**3.14.1[d]**	System flaws are reported within the specified time frame.
IA	Identification & Authentication			**3.14.1[e]**	The time within which to correct system flaws is specified.
IR	Incident Response			**3.14.1[f]**	System flaws are corrected within the specified time frame.
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SI.L2-3.14.2	Provide protection from malicious code at designated locations within organizational systems.	3.14.2[a]	Designated locations for malicious code protection are identified.
AT	Awareness & Training			3.14.2[b]	Protection from malicious code at designated locations is provided.
AU	Audit & Accountability	SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	3.14.3[a]	Response actions to system security alerts and advisories are identified.
CM	Configuration Management			3.14.3[b]	System security alerts and advisories are monitored.
IA	Identification & Authentication			3.14.3[c]	Actions in response to system security alerts and advisories are taken.
IR	Incident Response	SI.L2-3.14.4	Update malicious code protection mechanisms when new releases are available.	3.14.4[a]	Malicious code protection mechanisms are updated when new releases are available
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SI.L2-3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5[a]	The frequency for malicious code scans is defined.
AT	Awareness & Training			3.14.5[b]	Malicious code scans are performed with the defined frequency.
AU	Audit & Accountability			3.14.5[c]	Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection	SI.L2-3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	3.14.6[a]	The system is monitored to detect attacks and indicators of potential attacks.
PS	Personnel Security			3.14.6[b]	Inbound communications traffic is monitored to detect attacks and indicators of potential attacks.
PE	Physical Protection			3.14.6[c]	Outbound communications traffic is monitored to detect attacks and indicators of potential attacks.
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

Domain		CMMC Practice ID	Security Requirement		Assessment Objective
AC	Access Control	SI.L2-3.14.7	Identify unauthorized use of organizational systems	**3.14.7[a]**	Authorized use of the system is defined.
AT	Awareness & Training			**3.14.7[b]**	Unauthorized use of the system is identified.
AU	Audit & Accountability				
CM	Configuration Management				
IA	Identification & Authentication				
IR	Incident Response				
MA	Maintenance				
MP	Media Protection				
PS	Personnel Security				
PE	Physical Protection				
RA	Risk Assessment				
CA	Security Assessment & Authorization				
SC	System & Communications Protection				
SI	System & Information Integrity				

About C3

C3 accelerates CMMC cybersecurity compliance by designing, implementing, and managing IT & cybersecurity solutions purpose-built for the U.S. Defense Industrial Base.

C3 offers a wide range of compliance-centric managed IT services—from targeted services customized to fit within a client's existing environment to the C3 Suite, a set of packaged solutions, including fully managed CMMC offerings purpose-built to meet compliance requirements.

By rooting our prescriptive solutions in cybersecurity best practices and an intimate understanding of CMMC assessment requirements, the C3 Suite minimizes the risk of non-compliance and accelerates compliance timelines, enabling defense contractors to more easily achieve and maintain CMMC Level 2 compliance with confidence.

A leading provider of Microsoft 365 GCC High and Azure Government, C3 is a leading AOS-G Partner, a CMMC Registered Provider Organization (RPO), and one of the few companies to successfully support the DIBCAC assessment of a CMMC Third-Party Assessment Organization (C3PAO).

Visit us at: c3isit.com