Carnegie Mellon University
Software Engineering Institute

OVERVIEW OF PRACTICES AND PROCESSES OF THE CMMC ASSESSMENT GUIDES

Doug Gardner

February 2021

Introduction

This document is intended to help individuals unfamiliar with cybersecurity standards better understand the practices and processes of the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC).

The first section of the document lists the practice and process identifiers and descriptions in the CMMC Level 1 Assessment Guide and Level 3 Assessment Guide. A simple, concise explanation follow each identifier. The second section contains additional CMMC resources published by the Software Engineering Institute (SEI). Additional guidance for using both this document and the CMMC Assessment Guides is outlined in the blog posting *How to Use the CMMC Assessment Guides*. For more information about CMMC, visit the website of the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)).

CMMC Practices

Access Control (AC)

Level 1 AC Practices

Practice Identifier	AC.1.001
Description	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
In Other Words…	Manage permissions to get on a system or to connect your system to the network.

Go to All Practices

Practice Identifier	AC.1.002
Description	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
In Other Words…	Manage permissions to do specific things, limited by your role in the company.

Practice Identifier	AC.1.003
Description	Verify and control/limit connections to and use of external information systems.
In Other Words…	Demonstrate ways to trust systems that you don't own and can't control directly.

Practice Identifier	AC.1.004
Description	Control information posted or processed on publicly accessible information systems.
In Other Words…	Make sure you don't accidentally post sensitive information on your websites or social media.

Go to All Practices

Level 2 AC Processes

Practice Identifier	AC.2.999
Description	Establish a policy that includes Access Control.
In Other Words…	Have a policy that covers the scope of Access Control practices.

Practice Identifier	AC.2.998
Description	Document the CMMC practices to implement the Access Control policy.

In Other Words…	Document the procedures used to satisfy the Access Control practices.

Level 2 AC Practices

Practice Identifier	**AC.2.005**
Description	Provide privacy and security notices consistent with applicable CUI rules.
In Other Words…	Make sure users understand the terms of use for being on your company's sensitive systems and/or network.

Practice Identifier	**AC.2.006**
Description	Limit use of portable storage devices on external systems.
In Other Words…	Control how portable storage devices are used on your systems and network.

Practice Identifier	**AC.2.007**
Description	Employ the principle of least privilege, including for specific security functions and privileged accounts.
In Other Words…	Make sure users get access only to what they absolutely need to do their work.

Practice Identifier	**AC.2.008**
Description	Use non-privileged accounts or roles when accessing non-security functions.
In Other Words…	Control how your privileged accounts are used.

Go to All Practices

Practice Identifier	**AC.2.009**
Description	Limit unsuccessful logon attempts.
In Other Words…	Don't give an attacker unlimited tries to guess your passwords.

Practice Identifier	**AC.2.010**
Description	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
In Other Words…	Prevent people from reading information off an unattended computer.

Practice Identifier	AC.2.011
Description	Authorize wireless access prior to allowing such connections.
In Other Words…	Make sure wireless connections on your network are intentional and carefully managed.

Practice Identifier	AC.2.013
Description	Monitor and control remote access sessions.
In Other Words…	Make sure you know about and are managing anyone getting into your network from the outside.

Practice Identifier	AC.2.015
Description	Route remote access via managed access control points.
In Other Words…	Funnel your outside traffic through a small number of network access points.

Practice Identifier	AC.2.016
Description	Control the flow of CUI in accordance with approved authorizations.
In Other Words…	Understand and control how sensitive information moves through your network.

Level 3 AC Processes

Go to All Practices

Practice Identifier	AC.3.997
Description	Establish, maintain, and resource a plan that includes Access Control.
In Other Words…	Make sure the Access Control practices are thoroughly planned and adequately resourced.

Level 3 AC Practices

Practice Identifier	AC.3.017
Description	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
In Other Words…	Make sure key tasks are shared and distributed to limit the impact of insider misbehavior.

Practice Identifier	AC.3.018
Description	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
In Other Words…	Make sure no unauthorized people or processes are executing sensitive or privileged tasks.

Practice Identifier	AC.3.019
Description	Terminate (automatically) user sessions after a defined condition.
In Other Words…	Make and enforce rules to limit people camping out on your network.

Practice Identifier	AC.3.012
Description	Protect wireless access using authentication and encryption.
In Other Words…	Use available tools to restrict wireless access to your network.

Practice Identifier	AC.3.020
Description	Control connection of mobile devices.
In Other Words…	Manage mobile devices that connect to your network.

Go to All Practices

Practice Identifier	AC.3.014
Description	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
In Other Words…	Make sure attackers can’t read or manipulate data in transit between you and your remote partners.

Practice Identifier	AC.3.021
Description	Authorize remote execution of privileged commands and remote access to security-relevant information.
In Other Words…	Carefully manage the ability of remote users to execute sensitive or privileged functions.

Practice Identifier	**AC.3.022**
Description	Encrypt CUI on mobile devices and mobile computing platforms.
In Other Words…	Protect sensitive data on devices so it's not compromised if the device is lost or stolen.

Asset Management (AM)

Level 3 AM Processes

Go to All Practices

Practice Identifier	AM.2.999
Description	Establish a policy that includes Asset Management.
In Other Words…	Have a policy that covers the scope of the Asset Management practices.

Practice Identifier	AM.2.998
Description	Document the CMMC practices to implement the Asset Management policy.
In Other Words…	Document the procedures used to satisfy the Asset Management practices.

Practice Identifier	AM.3.997
Description	Establish, maintain, and resource a plan that includes Asset Management.
In Other Words…	Make sure the Asset Management practices are thoroughly planned and adequately resourced.

Level 3 AM Practices

Practice Identifier	AM.3.036
Description	Define procedures for the handling of CUI data.
In Other Words…	Have written policies that ensure that you manage and protect CUI data according to guidelines and regulations.

Audit and Accountability (AU)

Level 2 AU Processes

Go to All Practices

Practice Identifier	AU.2.999
Description	Establish a policy that includes Audit and Accountability.
In Other Words…	Have a policy that covers the scope of the Audit and Accountability practices.

Practice Identifier	AU.2.998
Description	Document the CMMC practices to implement the Audit and Accountability policy.
In Other Words…	Document the procedures used to satisfy the Audit and Accountability practices.

Level 2 AU Practices

Practice Identifier	AU.2.041
Description	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
In Other Words…	Make sure you can tie actions on your systems to individuals.

Practice Identifier	AU.2.042
Description	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.
In Other Words…	Create and store audit data with the goal of making sure it supports the investigation of system events.

Practice Identifier	AU.2.043
Description	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
In Other Words…	Time synchronize your systems to ensure audit data is comparable.

Go to All Practices

Practice Identifier	AU.2.044
Description	Review audit logs.
In Other Words…	Regularly reviewing audit logs is a good way to discover system issues quickly.

Level 3 AU Processes

Practice Identifier	AU.3.997
Description	Establish, maintain, and resource a plan that includes Audit and Accountability.
In Other Words…	Make sure the Audit and Accountability practices are thoroughly planned and adequately resourced.

Level 3 AU Practices

Practice Identifier	AU.3.045
Description	Review and update logged events.
In Other Words…	Review your audit generation strategy regularly to ensure that it meets your investigative requirements.

Practice Identifier	AU.3.046
Description	Alert in the event of an audit logging process failure.
In Other Words…	Configure your logging mechanisms to alert someone if the mechanisms aren't working properly.

Practice Identifier	AU.3.048
Description	Collect audit information (e.g., logs) into one or more central repositories.
In Other Words…	Managing logs on individual devices can be cumbersome. Use available tools to consolidate and manage logs centrally.

Go to All Practices

Practice Identifier	AU.3.049
Description	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
In Other Words…	Treat your collected audit data as highly sensitive and protect it accordingly.

Practice Identifier	AU.3.050
Description	Limit management of audit logging functionality to a subset of privileged users.
In Other Words…	Make sure the audit logging process covers privileged users by separating the audit review responsibilities from other privileged access roles.

Practice Identifier	AU.3.051
Description	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
In Other Words…	Combine data from all available security sources to support situational awareness.

Practice Identifier	AU.3.052
Description	Provide audit record reduction and report generation to support on-demand analysis and reporting.
In Other Words…	Use available tools to make raw audit data easier to work with, easier to combine with other data, and easier to turn into reports.

Awareness and Training (AT)

Level 2 AT Processes

Go to All Practices

Practice Identifier	AT.2.999
Description	Establish a policy that includes Awareness and Training.
In Other Words…	Have a policy that covers the scope of the Awareness and Training practices.

Practice Identifier	AT.2.998
Description	Document the CMMC practices to implement the Awareness and Training policy.
In Other Words…	Document the procedures used to satisfy the Awareness and Training practices.

Level 2 AT Practices

Practice Identifier	AT.2.056
Description	Ensure that managers, system 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.
In Other Words…	Make sure everyone in your company is trained on the basics of computer security, typically referred to as security awareness training.

Practice Identifier	AT.2.057
Description	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
In Other Words…	Make sure people in your company who have information security responsibilities are trained specifically in the security aspects of their duties.

Level 3 AT Processes

Go to All Practices

Practice Identifier	AT.3.997
Description	Establish, maintain, and resource a plan that includes Awareness and Training.
In Other Words…	Make sure the Awareness and Training practices are thoroughly planned and adequately resourced.

Level 3 AT Practices

Practice Identifier	AT.3.058
Description	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
In Other Words…	Train everyone in your company on the risks and indicators of insider threat.

Configuration Management (CM)

Level 2 CM Processes

Go to All Practices

Practice Identifier	CM.2.999
Description	Establish a policy that includes Configuration Management.
In Other Words…	Have a policy that covers the scope of the Configuration Management practices.

Practice Identifier	CM.2.998
Description	Document the CMMC practices to implement the Configuration Management policy.
In Other Words…	Document the procedures used to satisfy the Configuration Management practices.

Level 2 CM Practices

Practice Identifier	CM.2.061
Description	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
In Other Words…	Maintain a list of your hardware and software, including how they should be securely configured and the associated documentation (manuals, change logs, etc.).

Practice Identifier	CM.2.062
Description	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
In Other Words…	When configuring systems, limit services, applications, and functions to only those necessary to achieve the system's specified purpose.

Practice Identifier	CM.2.063
Description	Control and monitor user-installed software.
In Other Words…	Manage the ability of users to install software on their systems.

Go to All Practices

Practice Identifier	CM.2.064
Description	Establish and enforce security configuration settings for information technology products employed in organizational systems.
In Other Words…	Regularly check the configuration of your systems to make sure they have not drifted away from the security baseline.

Practice Identifier	CM.2.065
Description	Track, review, approve, or disapprove, and log changes to organizational systems.
In Other Words…	Make sure all configuration changes to company systems are reviewed, approved and documented.

Practice Identifier	CM.2.066
Description	Analyze the security impact of changes prior to implementation.
In Other Words…	Make changes to security settings only after carefully exploring the potential risks.

Level 3 CM Processes

Practice Identifier	CM.3.997
Description	Establish, maintain, and resource a plan that includes Configuration Management.
In Other Words…	Make sure the Configuration Management practices are thoroughly planned and adequately resourced.

Level 3 CM Practices

Practice Identifier	CM.3.067
Description	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
In Other Words…	Prevent unauthorized changes to your systems using physical access (locks, building access, etc.) and logical access (permissions, network segmentation, etc.) mechanisms.

Go to All Practices

Practice Identifier	CM.3.068
Description	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
In Other Words…	Learn what programs, ports, protocols, and services are required for your company operations and then remove or restrict everything else.

Practice Identifier	CM.3.069
Description	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.
In Other Words…	Control unwanted software execution on systems by having a policy that uses available tools to evaluate and approve software at runtime.

Identification and Authentication (IA)

Level 1 IA Practices

Go to All Practices

Practice Identifier	IA.1.076
Description	Identify information system users, processes acting on behalf of users, or devices.
In Other Words…	Develop processes for uniquely naming and identifying systems and users on your network so you can tell exactly which system or user is involved in a specific activity.

Practice Identifier	IA.1.077
Description	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
In Other Words…	Use strong authentication practices to make users, processes, and devices connecting to your systems or networks prove they are authorized.

Level 2 IA Processes

Practice Identifier	IA.2.999
Description	Establish a policy that includes Identification and Authentication.
In Other Words…	Have a policy that covers the scope of the Identification and Authentication practices.

Practice Identifier	IA.2.998
Description	Document the CMMC practices to implement the Identification and Authentication policy.
In Other Words…	Document the procedures used to satisfy the Identification and Authentication practices.

Level 2 IA Practices

Go to All Practices

Practice Identifier	IA.2.078
Description	Enforce a minimum password complexity and change of characters when new passwords are created.
In Other Words…	Make sure passwords are complex by using a variety of character types to make them difficult for attackers to guess.

Practice Identifier	IA.2.079
Description	Prohibit password reuse for a specified number of generations.
In Other Words…	Don't allow users to reuse passwords.

Practice Identifier	IA.2.080
Description	Allow temporary password use for system logons with an immediate change to a permanent password.
In Other Words…	Make sure temporary passwords are changed immediately.

Practice Identifier	IA.2.081
Description	Store and transmit only cryptographically-protected passwords.
In Other Words…	If a password must be stored or transmitted, use cryptographic tools to prevent it from being compromised.

Practice Identifier	IA.2.082
Description	Obscure feedback of authentication information.
In Other Words…	Protect against someone seeing you enter your password by covering the characters as they are entered.

Level 3 IA Processes

Practice Identifier	IA.3.997
Description	Establish, maintain, and resource a plan that includes Identification and Authentication.
In Other Words…	Make sure the Identification and Authentication practices are thoroughly planned and adequately resourced.

Level 3 IA Practices

Go to All Practices

Practice Identifier	IA.3.083
Description	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
In Other Words…	Require users to prove they are who they say they are using more than one technique: something you know (e.g., password), something you have (e.g., token), something you are (e.g., fingerprint).

Practice Identifier	IA.3.084
Description	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
In Other Words…	Choose authentication methods that are sophisticated enough to ensure that authentication information captured in transit cannot be reused at a later time.

Practice Identifier	IA.3.085
Description	Prevent the reuse of identifiers for a defined period.
In Other Words…	Don’t reuse user IDs or system names to ensure previous accesses are not inherited by the new instance.

Practice Identifier	IA.3.086
Description	Disable identifiers after a defined period of inactivity.
In Other Words…	Accounts that belonged to people who have left your organization offer attackers additional paths to compromise your network. Disable and delete these accounts as soon as possible.

Incident Response (IR)

Level 2 IR Processes

Go to All Practices

Practice Identifier	IR.2.999
Description	Establish a policy that includes Incident Response.
In Other Words…	Have a policy that covers the scope of the Incident Response practices

Practice Identifier	IR.2.998
Description	Document the CMMC practices to implement the Incident Response policy.
In Other Words…	Document the procedures used to satisfy the Incident Response practices.

Level 2 IR Practices

Practice Identifier	IR.2.092
Description	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
In Other Words…	Build a comprehensive capability to manage the security issues that arise through errors or attacks.

Practice Identifier	IR.2.093
Description	Detect and report events.
In Other Words…	Across your company, actively look for and share errors or oddities on your systems and networks.

Practice Identifier	IR.2.094
Description	Analyze and triage events to support event resolution and incident declaration.
In Other Words…	Analyze and categorize collected errors and oddities based on how threatening they are to your operations.

Go to All Practices

Practice Identifier	IR.2.096
Description	Develop and implement responses to declared incidents according to predefined procedures.
In Other Words…	Wargame possible cyber incidents, then create detailed response plans.

Practice Identifier	IR.2.097
Description	Perform root cause analysis on incidents to determine underlying causes.
In Other Words…	Figure out what happened in as much detail as possible, then update your policies and improve prevention techniques.

Level 3 IR Processes

Practice Identifier	IR.3.997
Description	Establish, maintain, and resource a plan that includes Incident Response.
In Other Words…	Make sure the Incident Response practices are thoroughly planned and adequately resourced.

Level 3 IR Practices

Practice Identifier	IR.3.098
Description	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
In Other Words…	Track and share (as required) progress of incidents as they move through the incident response process.

Practice Identifier	IR.3.099
Description	Test the organizational incident response capability.
In Other Words…	Practice your incident response processes to ensure everything goes as smoothly as possible when an incident occurs.

Maintenance (MA)

Level 2 MA Processes

Go to All Practices

Practice Identifier	MA.2.999
Description	Establish a policy that includes Maintenance.
In Other Words…	Have a policy that covers the scope of the Maintenance practices

Practice Identifier	MA.2.998
Description	Document the CMMC practices to implement the Maintenance policy.
In Other Words…	Document the procedures used to satisfy the Maintenance practices.

Level 2 MA Practices

Practice Identifier	MA.2.111
Description	Perform maintenance on organizational systems.
In Other Words…	Keep your systems up to date and operating as efficiently as possible.

Practice Identifier	MA.2.112
Description	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
In Other Words…	Think of maintenance activities as another potential attack vector and control them accordingly.

Practice Identifier	MA.2.113
Description	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
In Other Words…	If maintenance from the outside is necessary, require more than one authentication technique and limit maintenance duration.

Go to All Practices

Practice Identifier	MA.2.114
Description	Supervise the maintenance activities of personnel without required access authorization.
In Other Words…	Physically supervise and require focused, temporary credentials for maintenance personnel from the outside.

Level 3 MA Processes

Practice Identifier	MA.3.997
Description	Establish, maintain, and resource a plan that includes Maintenance.
In Other Words…	Make sure the Maintenance practices are thoroughly planned and adequately resourced.

Level 3 MA Practices

Practice Identifier	MA.3.115
Description	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
In Other Words…	Remove sensitive data from your systems if you have to send them off-site for maintenance.

Practice Identifier	MA.3.116
Description	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
In Other Words…	Because maintenance is a possible attack vector, make sure maintenance tools introduced from any source (vendor sites, script libraries, flash drives, etc.) are scanned for malware before you use them.

Media Protection (MP)

Level 1 MP Practices

Go to All Practices

Practice Identifier	MP.1.118
Description	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
In Other Words…	Don't let sensitive data go out with the trash.

Level 2 MP Processes

Practice Identifier	MP.2.999
Description	Establish a policy that includes Media Protection.
In Other Words…	Have a policy that covers the scope of the Media Protection practices

Practice Identifier	MP.2.998
Description	Document the CMMC practices to implement the Media Protection policy.
In Other Words…	Document the procedures used to satisfy the Media Protection practices.

Level 2 MP Practices

Practice Identifier	MP.2.119
Description	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
In Other Words…	Secure sensitive data in its various forms, including paper and when it's stored on non-networked physical devices.

Practice Identifier	MP.2.120
Description	Limit access to CUI on system media to authorized users.
In Other Words…	Protect access to sensitive data in its various forms, including paper and when it's stored on non-networked physical devices.

Go to All Practices

Practice Identifier	MP.2.121
Description	Control the use of removable media on system components.
In Other Words…	Secure sensitive data in its various forms, including when it's stored on removable physical devices.

Level 3 MP Processes

Practice Identifier	MP.3.997
Description	Establish, maintain, and resource a plan that includes Media Protection.
In Other Words…	Make sure the Media Protection practices are thoroughly planned and adequately resourced.

Level 3 MP Practices

Practice Identifier	MP.3.122
Description	Mark media with necessary CUI markings and distribution limitations.
In Other Words…	Follow the legal requirements to mark information as directed by the data owners.

Practice Identifier	MP.3.123
Description	Prohibit the use of portable storage devices when such devices have no identifiable owner.
In Other Words…	Prohibit all portable storage devices that you have not approved specifically for use.

Practice Identifier	MP.3.124
Description	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
In Other Words…	If you have to send sensitive data outside its usual location, provide appropriate physical protections and keep track of it at all times.

Practice Identifier	MP.3.125
Description	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
In Other Words…	If you have to send sensitive data outside its usual location, encrypt it and provide appropriate physical protections.

Go to All Practices

Personnel Security (PS)

Level 2 PS Processes

Go to All Practices

Practice Identifier	PS.2.999
Description	Establish a policy that includes Personnel Security.
In Other Words…	Have a policy that covers the scope of the Personnel Security practices

Practice Identifier	PS.2.998
Description	Document the CMMC practices to implement the Personnel Security policy.
In Other Words…	Document the procedures used to satisfy the Personnel Security practices.

Level 2 PS Practices

Practice Identifier	PS.2.127
Description	Screen individuals prior to authorizing access to organizational systems containing CUI.
In Other Words…	Evaluate each employee's trustworthiness before granting access to sensitive data.

Practice Identifier	PS.2.128
Description	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
In Other Words…	Keep your personnel records up to date to ensure that people who have left their positions or the company cannot access sensitive company or government information.

Level 3 PS Processes

Practice Identifier	PS.3.997
Description	Establish, maintain, and resource a plan that includes Personnel Security.
In Other Words…	Make sure the Physical Security practices are thoroughly planned and adequately resourced.

Physical Protection (PE)

Level 1 PE Practices

Go to All Practices

Practice Identifier	PE.1.131
Description	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
In Other Words…	Control who can get near your systems and networks.

Practice Identifier	PE.1.132
Description	Escort visitors and monitor visitor activity.
In Other Words…	Escort and monitor visitors to your facility.

Practice Identifier	PE.1.133
Description	Maintain audit logs of physical access.
In Other Words…	Keep track of who goes in and out of your facility to help investigate incidents.

Practice Identifier	PE.1.134
Description	Control and manage physical access devices.
In Other Words…	Control keys, combinations, and access cards to make sure they are not copied or shared.

Level 2 PE Processes

Practice Identifier	PE.2.999
Description	Establish a policy that includes Physical Protection.
In Other Words…	Have a policy that covers the scope of the Physical Protection practices.

Practice Identifier	PE.2.998
Description	Document the CMMC practices to implement the Physical Protection policy.
In Other Words…	Document the procedures used to satisfy the Physical Protection practices.

Level 2 PE Practices

Go to All Practices

Practice Identifier	PE.2.135
Description	Protect and monitor the physical facility and support infrastructure for organizational systems.
In Other Words…	Make sure it's not easy for someone to sneak or break into your facility or use power or cable lines to gain access to your sensitive information.

Level 3 PE Processes

Practice Identifier	PE.3.997
Description	Establish, maintain, and resource a plan that includes Physical Protection.
In Other Words…	Make sure the Physical Protection practices are thoroughly planned and adequately resourced.

Level 3 PE Practices

Practice Identifier	PE.3.136
Description	Enforce safeguarding measures for CUI at alternate work sites.
In Other Words…	Ensure that sensitive data is physically and logically protected at alternate work situations, such as work-from-home or satellite offices.

Recovery (RE)

Level 2 RE Processes

Go to All Practices

Practice Identifier	RE.2.999
Description	Establish a policy that includes Recovery.
In Other Words…	Have a policy that covers the scope of the Recovery practices

Practice Identifier	RE.2.998
Description	Document the CMMC practices to implement the Recovery policy.
In Other Words…	Document the procedures used to satisfy the Recovery practices.

Level 2 RE Practices

Practice Identifier	RE.2.137
Description	Regularly perform and test data backups.
In Other Words…	Make copies of your systems and data so you can rebuild them if necessary. Test them regularly to make sure they work.

Practice Identifier	RE.2.138
Description	Protect the confidentiality of backup CUI at storage locations.
In Other Words…	Make sure the copies of the systems and data you create cannot be deleted or tampered with.

Level 3 RE Processes

Practice Identifier	RE.3.997
Description	Establish, maintain, and resource a plan that includes Recovery.
In Other Words…	Make sure the Recovery practices are thoroughly planned and adequately resourced.

Level 3 RE Practices

Practice Identifier	RE.3.139
Description	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.
In Other Words…	Use available tools and follow stricter guidance for backing up sensitive systems.

Go to All Practices

Risk Management (RM)

Level 2 RM Processes

Go to All Practices

Practice Identifier	RM.2.999
Description	Establish a policy that includes Risk Management.
In Other Words…	Have a policy that covers the scope of the Risk Management practices

Practice Identifier	RM.2.998
Description	Document the CMMC practices to implement the Risk Management policy.
In Other Words…	Document the procedures used to satisfy the Risk Management practices.

Level 2 RM Practices

Practice Identifier	RM.2.141
Description	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.
In Other Words…	Build processes to regularly identify actions and events that can hurt your ability to perform your mission.

Practice Identifier	RM.2.142
Description	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
In Other Words…	Actively look for weaknesses in your systems and processes so you find them before an attacker does.

Practice Identifier	RM.2.143
Description	Remediate vulnerabilities in accordance with risk assessments.
In Other Words…	Fix identified problems in the order that they can hurt your ability to complete your company mission.

Level 3 RM Processes

Go to All Practices

Practice Identifier	RM.3.997
Description	Establish, maintain, and resource a plan that includes Risk Management.
In Other Words…	Make sure the Risk Management practices are thoroughly planned and adequately resourced.

Level 3 RM Practices

Practice Identifier	RM.3.144
Description	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
In Other Words…	Manage risk more systematically by introducing categories and metrics.

Practice Identifier	RM.3.146
Description	Develop and implement risk mitigation plans.
In Other Words…	Develop and put in place plans to address the most severe risks.

Practice Identifier	RM.3.147
Description	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.
In Other Words…	If you must continue using hardware or software that is no longer supported by the developer, manage it carefully and isolate it from other systems as much as possible.

Security Assessment (CA)

Level 2 CA Processes

Go to All Practices

Practice Identifier	CA.2.999
Description	Establish a policy that includes Security Assessment.
In Other Words…	Have a policy that covers the scope of the Security Assessment practices

Practice Identifier	CA.2.998
Description	Document the CMMC practices to implement the Security Assessment policy.
In Other Words…	Document the procedures used to satisfy the Security Assessment practices.

Level 2 CA Practices

Practice Identifier	CA.2.157
Description	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.
In Other Words…	Document your security activities so they are well understood and implemented consistently.

Practice Identifier	CA.2.158
Description	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
In Other Words…	Regularly review your security efforts to make sure they make sense and are working as intended.

Practice Identifier	CA.2.159
Description	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
In Other Words…	Document how you plan to close high-risk security gaps, then implement those plans.

Level 3 CA Processes

Go to All Practices

Practice Identifier	CA.3.997
Description	Establish, maintain, and resource a plan that includes Security Assessment.
In Other Words…	Make sure the Security Assessment practices are thoroughly planned and adequately resourced.

Level 3 CA Practices

Practice Identifier	CA.3.161
Description	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
In Other Words…	Monitor specific security actions as frequently as possible to make sure they are effective.

Practice Identifier	CA.3.162
Description	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.
In Other Words…	If you develop your own software to support your operations, make sure it is developed using software development practices that emphasize security.

Situational Awareness (SA)

Level 3 SA Processes

Go to All Practices

Practice Identifier	SA.2.999
Description	Establish a policy that includes Situational Awareness.
In Other Words…	Have a policy that covers the scope of the Situational Awareness practices.

Practice Identifier	SA.2.998
Description	Document the CMMC practices to implement the Situational Awareness policy.
In Other Words…	Document the procedures used to satisfy the Situational Awareness practices.

Practice Identifier	SA.3.997
Description	Establish, maintain, and resource a plan that includes Situational Awareness.
In Other Words…	Make sure the Situational Awareness practices are thoroughly planned and adequately resourced.

Level 3 SA Processes

Practice Identifier	SA.3.169
Description	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
In Other Words…	Connect with and use sources of current information about cyber threats, tools, techniques, and targets.

System and Communications Protection (SC)

Level 1 SC Practices

Go to All Practices

Practice Identifier	SC.1.175
Description	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
In Other Words…	Use available tools to create a protected barrier around your network and to separate internal portions of your network from each other.

Practice Identifier	SC.1.176
Description	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
In Other Words…	Separate your network to protect internal systems and activities from anything that has to interact regularly with outside (untrusted) entities.

Level 2 SC Processes

Practice Identifier	SC.2.999
Description	Establish a policy that includes System and Communications Protection.
In Other Words…	Have a policy that covers the scope of the Systems and Communications Protection practices.

Practice Identifier	SC.2.998
Description	Document the CMMC practices to implement the System and Communications Protection policy.
In Other Words…	Document the procedures used to satisfy the System and Communications Protection practices.

Level 2 SC Practices

Go to All Practices

Practice Identifier	SC.2.178
Description	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
In Other Words…	Protect yourself from electronic eavesdropping by reviewing the security aspects of whiteboards, cameras, microphones and other collaboration devices.

Practice Identifier	SC.2.179
Description	Use encrypted sessions for the management of network devices.
In Other Words…	Require encryption for all sensitive communications, especially those that involve remote administration.

Level 3 SC Processes

Practice Identifier	SC.3.997
Description	Establish, maintain, and resource a plan that includes System and Communications Protection.
In Other Words…	Make sure the Systems and Communications Protection practices are thoroughly planned and adequately resourced.

Level 3 SC Practices

Practice Identifier	SC.3.177
Description	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
In Other Words…	Use NIST-approved cryptography to secure your sensitive data.

Practice Identifier	SC.3.180
Description	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
In Other Words…	Make security an underlying foundation of other processes, such as network architecture, software development, and systems engineering.

Go to All Practices

Practice Identifier	SC.3.181
Description	Separate user functionality from system management functionality.
In Other Words…	Separate administrative systems and functions from functions that don't require elevated privileges.

Practice Identifier	SC.3.182
Description	Prevent unauthorized and unintended information transfer via shared system resources.
In Other Words…	Control shared resources (hard drives, network shares, collaboration software, etc.) so they don't get reused in a way that makes sensitive data available to unauthorized users.

Practice Identifier	SC.3.183
Description	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
In Other Words…	Block all incoming traffic, then only allow traffic after you are sure it is necessary to complete your mission.

Practice Identifier	SC.3.184
Description	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).
In Other Words…	Don't allow remote user systems to connect to your VPN and another network simultaneously. This will help prevent an attacker from another network from 'passing through' your user's system to attack your network.

Practice Identifier	SC.3.185
Description	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
In Other Words…	Use NIST-approved encryption to protect sensitive data as it moves around your network and between your network and other networks.

Go to All Practices

Practice Identifier	SC.3.186
Description	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
In Other Words…	Actively shut down connections between your network and the outside after a fixed time of inactivity or when there is no longer a need for the connection.

Practice Identifier	SC.3.187
Description	Establish and manage cryptographic keys for cryptography employed in organizational systems.
In Other Words…	Pay special attention to the management of cryptographic keys.

Practice Identifier	SC.3.188
Description	Control and monitor the use of mobile code.
In Other Words…	Implement a policy that tightly controls the execution of scripts downloaded from the Internet.

Practice Identifier	SC.3.189
Description	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
In Other Words…	Secure Voice-over-IP (VoIP) the same as any other internet-based application.

Practice Identifier	SC.3.190
Description	Protect the authenticity of communications sessions.
In Other Words…	Add mechanisms to ensure that users and partners really are who they say they are when they communicate on your network.

Practice Identifier	SC.3.191
Description	Protect the confidentiality of CUI at rest.
In Other Words…	Protect sensitive data when it is stored anywhere on your network.

Go to All Practices

Practice Identifier	SC.3.192
Description	Implement Domain Name System (DNS) filtering services.
In Other Words…	Take advantage of services that keep track of malicious actors and sites on the Internet and use their information to prevent your users from going to high-risk areas.

Practice Identifier	SC.3.193
Description	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).
In Other Words…	Develop training and processes to ensure that sensitive data doesn't end up published on your employees' social media accounts.

System and Information Integrity (SI)

Level 1 SI Practices

Go to All Practices

Practice Identifier	SI.1.210
Description	Identify, report, and correct information and information system flaws in a timely manner.
In Other Words…	Bad news doesn't get better with age. Have a process to quickly report and mitigate vulnerabilities and weaknesses as soon as they are identified.

Practice Identifier	SI.1.211
Description	Provide protection from malicious code at appropriate locations within organizational information systems.
In Other Words…	Build a defense program for your network aimed at preventing, detecting, and removing malicious code.

Practice Identifier	SI.1.212
Description	Update malicious code protection mechanisms when new releases are available.
In Other Words…	Commercial security products attempt to keep up with specific and general Internet threats. So, you should stay up-to-date with their releases of new software, attack signatures, and reputation assessments.

Practice Identifier	SI.1.213
Description	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
In Other Words…	Assume that files coming in from the outside are malicious and check them before introducing them onto your network. Periodically check files on your systems to look for malicious code that has slipped past your other defenses.

Level 2 SI Processes

Go to All Practices

Practice Identifier	SI.2.999
Description	Establish a policy that includes System and Information Integrity.
In Other Words…	Have a policy that covers the scope of the System and Information Integrity practices.

Practice Identifier	SI.2.998
Description	Document the CMMC practices to implement the System and Information Integrity policy.
In Other Words…	Document the procedures used to satisfy the System and Information Integrity practices.

Level 2 SI Practices

Practice Identifier	SI.2.214
Description	Monitor system security alerts and advisories and take action in response.
In Other Words…	Actively seek out and subscribe to trusted services that can give you advance warning about potential threats. Use the information they provide to be proactive in protecting your network.

Practice Identifier	SI.2.216
Description	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
In Other Words…	It's not enough to set up processes to monitor your network for possible threats. You have to continuously review the output of those processes, then act quickly on actual threats you find.

Practice Identifier	SI.2.217
Description	Identify unauthorized use of organizational systems.
In Other Words…	Use available tools to identify when a person or process is not behaving according to the rules or within acceptable norms.

Level 3 SI Processes

Go to All Practices

Practice Identifier	SI.3.997
Description	Establish, maintain, and resource a plan that includes System and Information Integrity.
In Other Words…	Make sure the System and Information Integrity practices are thoroughly planned and adequately resourced.

Level 3 SI Practices

Practice Identifier	SI.3.218
Description	Employ spam protection mechanisms at information system access entry and exit points.
In Other Words…	Spam is more than a nuisance – it can be a vector for attacks. Use available tools to reduce or eliminate it.

Practice Identifier	SI.3.219
Description	Implement email forgery protections.
In Other Words…	Make sure sensitive or high-level emails are protected from impersonation and forgery.

Practice Identifier	SI.3.220
Description	Utilize sandboxing to detect or block potentially malicious email.
In Other Words…	Use available tools to test threatening files and links prior to delivery to your users.

CMMC Resources

For additional information about CMMC and the CMMC Assessment Guides, consult the following Software Engineering Institute resources.

Table 1: CMMC Resources

Title	Type
CMMC—Securing the DIB Supply Chain	Web Page
An Introduction to the Cybersecurity Maturity Model Certification (CMMC)	Blog Post
Cybersecurity Maturity Model Certification (CMMC) Part 2: Process Maturity's Role in Cybersecurity	Blog Post
CMMC—Securing the DIB Supply Chain with the Cybersecurity Maturity Model Certification Process	Fact Sheet
The DoD's Cybersecurity Maturity Model Certification and Process Maturity	Webinar
CMMC Levels 1-3: Going Beyond NIST SP-171	Podcast
Reviewing and Measuring Activities for Effectiveness in CMMC Level 4	Podcast
Optimizing Process Maturity in CMMC Level 5	Podcast
Follow the CUI: 4 Steps to Starting Your CMMC Assessment	Blog Post
Follow the CUI: Setting the Boundaries for Your CMMC Assessment	Webinar
Hitting the Ground Running: Reviewing the 17 CMMC Level 1 Practices	Webinar
Beyond NIST SP 800-171: 20 Additional Practices in CMMC	Blog Post
Documenting Process for CMMC	Podcast
Building the Cybersecurity Maturity Model Certification	Article
Developing an Effective CMMC Policy	Podcast
CMMC Scoring	Fact Sheet
CMMC Scoring 101	Podcast
An Introduction to CMMC Assessment Guides	Podcast
The CMMC Level 1 Assessment Guide: A Closer Look	Podcast
The CMMC Level 3 Assessment Guide: A Closer Look	Podcast
How to Use the CMMC Assessment Guides	Blog Post

Go to All Practices

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0005