RISK ADVISORS

CMMC Maturity Level 1 (ML1)

Questionnaire

Version 1.2

Ric Daza, PhD – Managing Director
RD Risk Advisors, LLC.
CCIE^2, CISSP, CRISC, CISA, ISO 27K Lead Auditor
Cybersecurity Executive + Consultant Leading through Research + Education
ric@rdadvisors.co

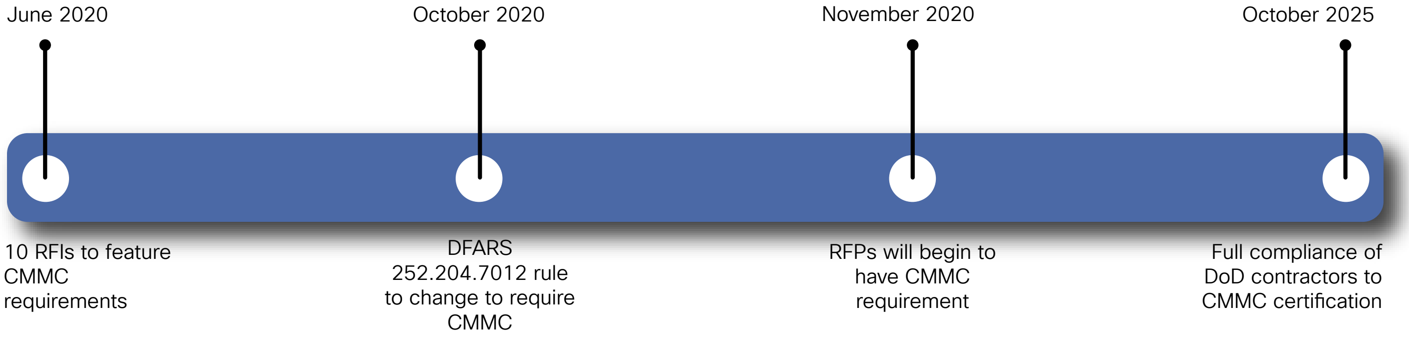
Maturity Level 1 (ML1) Preparation Questionnaire

Maturity Level 1 (ML1) Resource for PTACs

On 19 Feb 2020, the Defense Logistics Agency grants officer tasked the PTAC program managers with assisting their Defense Industrial Base (DIB) contractors to “step through” Cybersecurity Maturity Model Certification (CMMC) Maturity Level 1 (ML1) requirements, “as they are not highly technical requirements.”

Since then, COVID-19 pandemic has closed offices, and no further guidance has come to the PTAC community on this. RD Risk Advisors built this questionnaire for the PTAC community to assist their clients towards ML1.

For planning purposes keep in mind the timeline below, CMMC is scheduled to become required for DoD contracts in October and can begin appearing in RFPs in November. CMMC is already mentioned on the DoD SBIR 2020 BAAs and the NIH CIO sp4 draft RFP. In the final RFP for GSA STARS III - $50B Government Wide Acquisition Contract (GWAC) for 8a small businesses.


June 2020

10 RFIs to feature CMMC requirements

October 2020

DFARS 252.204.7012 rule to change to require CMMC

November 2020

RFPs will begin to have CMMC requirement

October 2025

Full compliance of DoD contractors to CMMC certification

Contract Award Process

1. Contracting Officer reviews contract requirements to determine which CMMC Level will be required
2. RFI posted including required CMMC level for bidding (may contain various levels to account for subcontracting flow-downs)
3. RFP released
4. Contractors submit proposals for RFP
5. Contracting Officer reviews proposals, awards contract, and CMMC certification must be presented at time of award by Contractor

Planning and budgeting for CMMC - certification ahead of time of contract award is critical. The majority of Small/Medium businesses in the Defense Industrial Base (DIB) have no formal yearly budget set aside for Information Technology (IT) - or for CMMC. It is encouraged that the business research its IT spend for the last 3 years (hardware, software, connectivity, subscriptions, services) to realize what is being spent on IT today.

Amount for IT Spend of Last 3 Years:

For planning purposes at ML1, a budget of 1% - 2% of DoD yearly gross revenue can be used to plan for both IT and CMMC spending combined.

Amount for Average Yearly Gross Revenue of DoD Contracts for Past 3 Years:

It has been documented that CMMC would be an “allowable cost” in DoD contracts:

> “The required CMMC level will be contained in sections L & M of the Request for Proposals (RFP) making cybersecurity an ‘allowable cost’ in DoD contracts.”
>
> “The cost of certification will be considered an allowable, reimbursable cost and will not be prohibitive. For contracts that require CMMC you may be disqualified from participating if your organization is not certified.”

Maturity Level 1 (ML1) Preparation Questionnaire

Best guess on how this would happen would be in section B of an RFP:

> "Cost Reimbursement is defined under FAR Subpart 16.3, Cost-Reimbursement Contracts. FAR Part 30, Cost Accounting Standards Administration and FAR Part 31, Contract Cost Principles and Procedures, may apply to cost-reimbursement Task Orders (TO). The contractor shall have and maintain an acceptable accounting system that will permit timely development of all necessary cost data in the form required by the proposed contract type. The contractor may be required to submit a cost proposal with supporting information for each cost element, including, but not limited to, direct labor, fringe benefits, overhead, general and administrative (G&A) expenses, facilities capital cost of money, other direct costs, and fee consistent with its cost accounting system, provisional billing rates, forward pricing rate agreements, and/or Cost Accounting Standards (CAS)."

Preliminary Work: Identify target maturity level

To determine the target maturity level, a contractor needs to review the current contracts and programs they'd like to bid on in the future. Remember the three pillars of a project being cost, performance, and schedule? Well, now a fourth one has been added – Cybersecurity.

ML1 is required for all DIB contractors. If a contract requires access to Controlled Unclassified Information (CUI), the contractor will be required to certify to ML3. So ensuring an organization should be pursuing ML1 and not ML3 should be done.

Maturity Level 3 - If a contractor receives or generates Controlled Unclassified Information, CUI - they must be certified at ML3. Contractors will need to carefully evaluate if they receive, handle, or generate other CUI and where that information is stored. More information about identifying CUI is maintained by the National Archives and Records Administration (NARA) at: https://www.archives.gov/cui/registry/category-list. A quick way for contractors to determine their necessary maturity level is to confirm if they currently work on projects requiring ITAR compliance. If they do, those contractors would need to target Level 3 of the CMMC standard, at a minimum, since ITAR data is considered CUI.

Questions:

Do current contracts require access to CUI?

Do future contracts require access to CUI?

What information is exchanged with Primes or DoD?

ML1 consists of processes performed and practices performed in an ad-hoc manner that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21. Documentation may or may not be relied upon - but documentation is often the cheapest and easiest way to satisfy a control.

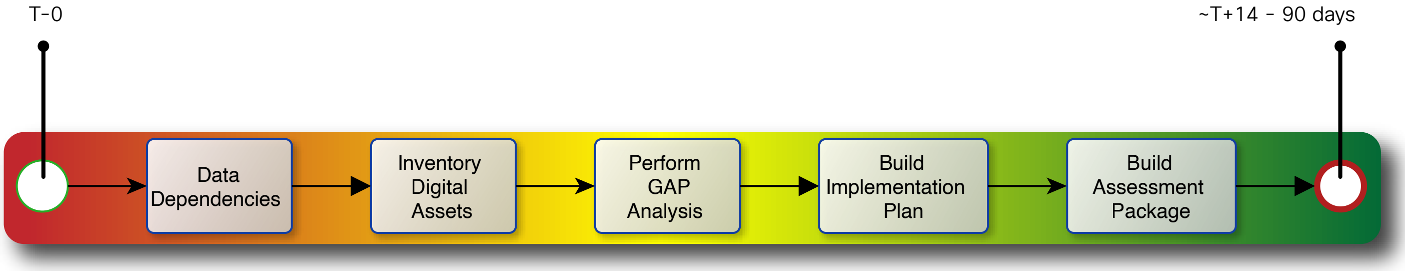
Maturity Level 1 - FAR Clause 52.204-21 corresponds to 17 requirements in CMMC ML1. ML1 is concerned with protecting Federal Contract Information (FCI), which is information from the Government provided under a contract - this means that contractors don't have FCI until after a contract has been awarded. If your company has a current DoD contract, then FCI could expect to be found in the following systems:

- Any systems that process or store email from government addresses
- Any systems that store files that are received from the government - this can be segmented by contract, policy, and technical controls so that FCI from contracts don't mix with other file storage.
- Hard storage of FCI data such as USB thumb drives, DVD, etc.
- Messaging, conference, and other systems that are used to transmit data from the government
- Any client workstation or device that access or store FCI data through email, files, messaging, or other means
- Any manufacturing devices that use or store FCI data
- Back-up and administrative systems that manage FCI systems
- Networks used by the above systems

These systems in your company probably have FCI, and should be included in the scope of a CMMC ML1 audit.

Maturity Level 1 (ML1) Preparation Questionnaire

A methodology makes it easier to work towards CMMC certification. Here is our methodology and timeline estimate for achieving ML1 (Not including the C3PAO assessment):



Step 1: Data Dependencies

Every cybersecurity effort must begin with understanding what needs to be protected, and its relative importance - what pilots call situational awareness. Cybersecurity's mission is to both protect an organization's ability to create value and protect the digital assets that are of value to an organization or its business partners such as CUI, FCI, or Intellectual Property (IP). A control is dependent on certain information about how the organization does business to determine if it is properly configured to mitigate the risk(s) and ultimately for certification. Business processes and their information flows are key things to document in this step.

The steps below are to assist PTACs with guiding their clients to CMMC Maturity Level 1 (ML1) Certification. Each CMMC domain/ control in ML1 is listed, along with the objective for the control, items that may be examined by an auditor, people that may be interviewed by an auditor, and tests that may be conducted. The domains are taken straight from CMMC Model V1.2 appendix B at https://www.acq.osd.mil/cmmc/draft.html, with control objectives, items examined, people that may be interviewed, and tests that may be conducted on each control are from NIST SP 800-171a at https://csrc.nist.gov/publications/detail/sp/800-171a/final

ACCESS CONTROL DOMAIN

AC.1.001 - Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems.
CMMC Clarification - Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up systems so that unauthorized users and devices cannot get on the company network.
Objectives for this control: Determine if authorized users are identified, processes acting on behalf of authorized users are identified, devices and other systems authorized to connect to the system are identified, system access is limited to authorized users, systems access is limited to processes acting on behalf of authorized users, system access is limited to authorized devices,
Things that may be examined for ML1: System configuration settings, list of active system accounts, name of individuals associated with each account, record of recently transferred, separated or terminated employees, list of conditions for group and role membership, list of recently disable system accounts along with the name of individual associated with each account, account management compliance reviews, system audit logs and records, list of devices and systems authorized to connect to organizational systems.
People that may be interviewed for ML1: Personnel with account management responsibilities, system or network administrators, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for managing system accounts, mechanisms for implementing account management

Questions:

What is the process to designate users with FCI access?

Are users with FCI access formally identified today?

Maturity Level 1 (ML1) Preparation Questionnaire

What mechanism does your business use to control/monitor access? (Workstation security, Active Directory, Box, Google, none)

AC.1.002 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
CMMC Clarification - Limit users/employees to only the information systems, roles, or applications they are permitted to use and that are needed for their jobs.
Objectives for this control: Determine if the types of transactions and functions that authorized users are permitted to execute are defined, system access is limited to the defined types of transactions and function for authorized users
Things that may be examined for ML1: procedures addressing access enforcement, list of approved authorization including remote access, system audit logs and records, system configuration settings
People that may be interviewed for ML1: Personnel with access enforcement responsibilities, system or network administrators, personnel with information security responsibilities, systems developers
Tests that may be conducted for ML1: Mechanisms implementing access control policy

Questions:

What is the process to designate FCI users level of access?

How are FCI users authorized before accessing FCI data?

What mechanism does your business use to control/monitor access? (Workstation security, Active Directory, Box, Google, none)

AC.1.003 - Verify and control/limit connections to and use of external information systems.
CMMC Clarification - Control and manage connections between your company network and outside network, such as the Internet or a network that doesn't belong to the company. Be aware of applications that can be run by outside systems. Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information. Limit how and when network is connected to outside systems and/or only certain employees can connect to outside systems from network resources.
Objectives for this control: Determine if connections to external systems are identified, the use of external systems is identified, connection to external systems are verified, the use of external systems is verified, connections to external systems are controlled/limited, the use of external systems is controlled/limited
Things that may be examined for ML1: procedures addressing the use of external systems, terms and conditions for external systems, list of applications accessible from external systems, system configuration settings, system connection or processing agreements
People that may be interviewed for ML1: Personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems, system or network administrators, personnel with information security responsibilities
Tests that may be conducted for ML1: Mechanisms implementing terms and conditions on use of external systems

Questions:

What is the process to designate devices with access to FCI data?

How are devices authorized before accessing FCI data?

What is the mechanism your business uses to control/monitor connections between networks that contain FCI data and other networks? (firewall, etc)

Maturity Level 1 (ML1) Preparation Questionnaire

AC.1.004 - Control information posted or processed on publicly accessible information systems.
CMMC Clarification - Don't allow sensitive information, including Federal Contract Information (FCI), which may include CUI, to become public. Know which users/employees are allowed to publish information on publicly accessible systems, like a company website. Limit and control information that is posted publicly.
Objectives for this control: Determine if individuals authorized to post or process information on publicly accessible systems are identified, procedures to ensure FCI is not posted or processed on identified publicly accessible systems
Things that may be examined for ML1: procedures addressing publicly accessible content, list of users authorized to post publicly accessible content on organization systems, system audit logs
People that may be interviewed for ML1: Personnel with responsibilities for managing publicly accessible information posted on organizational systems, personnel with information security responsibilities
Tests that may be conducted for ML1: Mechanisms implementing management of publicly accessible content

Questions:

What is the process to designate what data can be posted on public facing devices?

How are publicly accessible devices separated from devices processing FCI?

What is the mechanism used to manage publicly accessible content?

IDENTIFICATION AND AUTHENTICATION DOMAIN

IA.1.076 - Identify information system users, processes acting on behalf of users, or devices.
CMMC Clarification - Authentication helps you to know who is using or viewing your system. Make sure to assign individual, unique identifiers, like user names, to all employees/users who access company systems. Confirm the identities of users, processes, or devices before allowing them access to the company's information system-usually done through passwords.
Objectives for this control: Determine if system users are identified, processes acting on behalf of users are identified, devices accessing the system are identified
Things that may be examined for ML1: Procedures addressing user identification and authentication, system configuration settings, system audit logs, list of system accounts
People that may be interviewed for ML1: Personnel with system operations responsibilities, personnel with information security responsibilities, system or network administrators, personnel with account management responsibilities, system developers
Tests that may be conducted for ML1: Organizational processes for uniquely identifying and authenticating users, mechanisms supporting or implementing identification and authentication capability

Questions:

What is the process to identify users and processes of FCI data?

Is a unique identifier for each user accessing FCI data created?

What is the mechanism used to manage identification for users of FCI data?

Maturity Level 1 (ML1) Preparation Questionnaire

IA.1.077 - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
CMMC Clarification - Before you let a person or a device have access to your system, you need to verify that the user or device is who or what it claims to be. This verification is called authentication. The most common way to verify identity is using a username and a hard-to-guess password.
Some devices ship with default usernames and passwords. For example, some devices ship so that when you first logon to the device, the username is “admin” and the password is “admin”. When you have devices with this type of default username and password, you need to change the default password to a unique password you create. Default passwords are well known to the public, and easily found in a search. So, these default passwords would be easy for an unauthorized person to guess and use to gain access to your system.
Objectives for this control: Determine if the identity of each user is authenticated or verified as a prerequisite to system access, the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access, the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.
Things that may be examined for ML1: procedures addressing authenticator management, procedures addressing user identification and authentication, list of system authenticator types, system configuration settings, change control records associated with managing system authenticators, system audit logs
People that may be interviewed for ML1: Personnel with authenticator management responsibilities, personnel with information security responsibilities, system or network administrators
Tests that may be conducted for ML1: Mechanisms supporting or implementing authenticator management capability

Questions:

What is the process to designate what data can be posted on public facing devices?

How are publicly accessible devices separated from devices processing FCI?

What is the mechanism used to manage publicly accessible content?

MEDIA PROTECTION DOMAIN

MP.1.118 - Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
CMMC Clarification - In this case, “media” can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones. It is important to see what information is on these types of media. If there is Federal contract information (FCI)—information you or your company got doing work for the Federal government that is not shared publicly)—you or someone in your company should do one of two things before throwing the media away:

- clean or purge the information, if you want to reuse the device; or
- shred or destroy the device so it cannot be read.

Objectives for this control: Determine if system media containing FCI is sanitized or destroyed before disposal, system media containing FCI is sanitized before it is released for reuse.
Things that may be examined for ML1: Procedures addressing media sanitization and disposal, applicable standards and policies addressing media sanitization, media sanitization record, system audit logs, system configuration setting
People that may be interviewed for ML1: personnel with media sanitization responsibilities, personnel with information security responsibilities, system or network administrators
Tests that may be conducted for ML1: Organization processes for media sanitization, mechanisms supporting or implementing media sanitization

Questions:

Do you use media such as USB Keys, DVD’s, CD’s, etc for FCI data?

What is the process to sanitize or destroy media before disposal or reuse?

Maturity Level 1 (ML1) Preparation Questionnaire

What is the mechanism used to manage use of media on the FCI network?

PHYSICAL PROTECTION DOMAIN

PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
CMMC Clarification - Think about what parts of your physical space (e.g., office, plant, factory), what equipment, including the network, need to be protected from physical contact. For those parts of your company to which you want only specific employees to have physical access, monitor or limit who is able to enter those spaces with badges, key cards, etc.
Objectives for this control: Determine if authorized individuals allowed physical access are identified, physical access to organizational systems is limited to authorized individuals, physical access to equipment is limited to authorized individuals, physical access to operating environments is limited to authorized individuals
Things that may be examined for ML1: Procedures addressing physical access authorizations, authorized personnel access list, authorization credentials, physical access list reviews, physical access termination records
People that may be interviewed for ML1: Personnel with physical access authorization responsibilities, personnel with physical access to system facility, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access authorizations, mechanisms supporting or implementing physical access authorizations

Questions:

Is there a list of hardware used for FCI, and the locations of that hardware?

Are public locations of FCI hardware controlled/shielded from public view?

Are locations hosting FCI network hardware locked from public access, with access controlled?

PE.1.132 - Escort visitors and monitor visitor activity.
CMMC Clarification - Do not allow visitors, even those people you know well, to walk around your facility without an escort. Make sure that all non-employees wear special visitor badges and/or are escorted by an employee at all times while on your property.
Objectives for this control: Determine if visitors are escorted, visitor activity is monitored
Things that may be examined for ML1: Procedures addressing physical access control, physical access control logs or records, inventory records of physical access control devices, system entry and exit point, records of key and lock combination changes, storage locations for physical access control devices, physical access control devices, list of security safeguards, controlling access to designated publicly accessible areas within facility
People that may be interviewed for ML1: Personnel with physical access control responsibilities, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access control, mechanisms supporting or implementing physical access control, physical access control devices

Questions:

What is the process to escort/monitor visitor activity to areas processing FCI?

Are facility entry/exit points controlled?

What mechanisms are used to control/manage physical access?

Maturity Level 1 (ML1) Preparation Questionnaire

PE.1.133 - Maintain audit logs of physical access.
CMMC Clarification - Make sure you have a record of who is accessing both your facility (e.g., office, plant, factory) and your equipment. You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility.
Objectives for this control: Determine if audit logs of physical access are maintained
Things that may be examined for ML1: Physical and environmental protection policy, procedures addressing physical access control, physical access control logs, inventory records of physical access control devices, system entry and exit point, records of key and lock combination changes, storage locations for physical access control devices, physical access control devices, list of security safeguards controlling access to designated publicly accessible areas within facility
People that may be interviewed for ML1: Personnel with physical access control responsibilities, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access control, mechanisms supporting or implementing physical access control, physical access control devices

Questions:

What is the procedure for recording visitor access?

Where are visitor logs kept and for how long?

What mechanisms are used to record physical access?

PE.1.134 - Control and manage physical access devices.
CMMC Clarification - Controlling physical access devices like locks, badging, key cards, etc, are just as important as monitoring and limiting who is able to physically access certain equipment. Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.
Objectives for this control: Determine if physical access devices are identified, physical access devices are controlled, physical access devices are managed
Things that may be examined for ML1: Procedures addressing physical access control, physical access control logs, , inventory records of physical access control devices system entry and exit points, records of key and lock combination changes, storage locations for physical access control devices, physical access control devices, list of security safeguards controlling access to designated publicly accessible areas within facility
People that may be interviewed for ML1: Personnel with physical access control responsibilities, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access control, mechanisms supporting or implementing physical access control, physical access control devices

Questions:

What is the process to control physical access devices, keys, and locks?

Are badges controlled, keys controlled, locks/combination changed on a regular schedule?

What mechanisms are used to manage physical access?

Maturity Level 1 (ML1) Preparation Questionnaire

SYSTEM & COMMUNICATIONS PROTECTION DOMAIN

SC.1.175 - 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.
CMMC Clarification - Just as your office or plant has fences and locks for protection from the outside, and uses badges and keycards to keep non-employees out, your company's IT network or system has boundaries that must be protected. Many companies use a web proxy and a firewall.
Objectives for this control: Determine if the external system boundary is defined, key internal system boundaries are defined, communications are monitored at the external system boundary, communications are monitored at key internal boundaries, communications are controlled at the external system boundary, communications are controlled at key internal boundaries, communications are protected at the external system boundary, communications are protected at key internal boundaries
Things that may be examined for ML1: Procedures addressing boundary protection, list of key internal boundaries of the system, system design documentation, boundary protection hardware and software, system audit logs, system configuration settings
People that may be interviewed for ML1: System or network administrators, personnel with information security responsibilities, system developer, personnel with boundary protection responsibilities
Tests that may be conducted for ML1: Mechanisms implementing boundary protection capability

Questions:

What is the procedure to control system boundaries and communications?

Is there a list of system boundaries?

What mechanisms are used to manage system boundaries?

SC.1.176 - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
CMMC Clarification - Separate the publicly accessible systems from the internal systems that need to be protected. Do not place the internal systems on the same network as the publicly accessible systems. A network or part of a network that is separated (sometimes physically) from an internal network is called a demilitarized zone (DMZ). A DMZ is a host or part of a network put in a "neutral zone" between an organization's internal network (the protected side) and a larger network, like the Internet. To separate a subnetwork physically, your company may put in boundary control devices (i.e., routers, gateways, firewalls). This can also be done on a cloud network that can be separated from the rest of the network. A DMZ can add an extra layer of security to your company's LAN, because an external network node can reach only what is permitted to be accessed in the DMZ. Physical separation might involve a separate network infrastructure, dedicated network equipment with separate LAN segments and a firewall between the internal network and the DMZ segment and a firewall between the DMZ segment and the Internet. A logical separation might involve VLAN separation for the DMZ supporting a separate subnet with routing and access controls between subnets.
Objectives for this control: Determine if publicly accessible system components are identified, subnetworks for publicly accessible system components are physical or logically separated from internal networks
Things that may be examined for ML1: Procedures addressing boundary protection, list of key internal boundaries of the system, boundary protection hardware and software, system configuration settings, system audit logs
People that may be interviewed for ML1: System or network administrators, personnel with information security responsibilities, system developer, personnel with boundary protection responsibilities
Tests that may be conducted for ML1:

Questions:

What is the process to separate publicly accessible networks from FCI networks?

Does your business have guest wireless? IP phones, IP cameras, IP physical access control, etc?

Maturity Level 1 (ML1) Preparation

What mechanism(s) are used to manage subnetworks? (Routers, switches, firewalls)

SYSTEM & INFORMATION INTEGRITY DOMAIN

SI.1.210 - Identify, report, and correct information and information system flaws in a timely manner.
CMMC Clarification - All software and firmware have potential flaws. Many vendors work to reduce those flaws by releasing vulnerability information and updates to their software and firmware. Organizations should have a process to review relevant vendor newsletters with updates about common problems or weaknesses. After reviewing the information the organization should execute a process called patch management that allows for systems to be updated without adversely affecting the organization. Organizations should also purchase support from their vendors to ensure timely access to updates.
Objectives for this control: Determine if the time within which to identify systems flaws is specified, system flaws are identified within the specified time frame, the time within which to report system flaws is specified, system flaws are reported within the specified time frame, the time within which to correct system flaws is specified, system flaws are corrected within the specified time frame
Things that may be examined for ML1: Procedures addressing flaw remediation, procedures addressing configuration management, list of flaws and vulnerabilities potentially affecting the system, list of recent security flaw remediation actions performed on the system (installed patches, service packs, hot fixes, etc), test results from the installation of stowage and firmware updates to correct system flows, installation/change control records for security relevant software and firmware updates
People that may be interviewed for ML1: System or network administers, personnel with information security responsibilities, personnel installing, configuring, and maintaining the system, personnel with responsibility for flaw remediation, personnel with configuration management responsibility
Tests that may be conducted for ML1: Organizational processes for identifying, reporting and correcting system flaws, organization process for installing software and firmware updates, mechanisms support or implementing reporting, and correcting system flaws, mechanisms supporting or implementing testing software and firmware updates

Questions:

What is the process to document FCI information flows?

Does your business monitor vendor information for system flows?

What mechanisms are used to patch systems?

Maturity Level 1 (ML1) Preparation Questionnaire

SI.1.211 - Provide protection from malicious code at appropriate locations within organizational information systems.
CMMC Clarification - You can protect your company's valuable IT system by stopping malicious code at designated locations in your system. Malicious code is program code that purposefully creates an unauthorized function or process that will have a negative impact on the confidentiality, integrity, or availability of an information system. A designated location may be your network device or your computer.
Malicious code includes the following, which can be hidden in email, email attachments, web access:

- viruses, programs designed to damage, steal information, change data, send email, show messages, or any combination of these things;
- spyware, a program designed to gather information about a person's activity in secret, and is usually installed without the person knowing when they click on a link; and
- a trojan horse, a type of malware made to look like legitimate/real software, and used by cyber criminals to get access to a company's systems.

By using anti-malware tools, you can stop or lessen the impact of malicious code.
Objectives for this control: Determine if designated locations for malicious code protection are identified, protection from malicious code at designated is provided
Things that may be examined for ML1: configuration management procedures, procedures addressing malicious code protection, records of malicious code protection updates, malicious code protection mechanisms, system configuration settings , record of action initiated by malicious code protection mechanisms in response to malicious code detection, scan results from malicious code protection mechanisms, system audit logs
People that may be interviewed for ML1: System or network administrators, personnel with information security responsibilities, personnel installing, configuring, and maintaining the system, personnel with responsibility for malicious code protection, personnel with configuration management responsibility
Tests that may be conducted for ML1: Organizational processes for employing, updating, and configuring malicious code protection mechanisms, organization process for addressing false positives and configuring malicious code protection mechanisms, mechanisms supporting or implementing malicious code scanning and subsequent actions

Questions:

What is the procedure to note locations of FCI processing for malware protection?

Is anti-malware software installed on all FCI devices?

What mechanism is used to manage malware?

SI.1.212 - Update malicious code protection mechanisms when new releases are available.
CMMC Clarification - You can protect your company's valuable IT systems by staying up to date on new security releases that stop malicious code and monitoring the system regularly. Malicious code is program code that is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.
Objectives for this control: Determine if malicious code protection mechanisms are updated when new releases are available
Things that may be examined for ML1: Procedures addressing malicious code protection, malicious code protection mechanisms, records of malicious code protection updates, system configuration settings, scan results from malicious code protection mechanisms, record of actions initiated by malicious code protection mechanisms in response to malicious code detection, system audit logs
People that may be interviewed for ML1: Personnel with security alert and advisory responsibilities, personnel implement, operating, maintain, and using the system, personnel, organization elements, and external organizations to whom alerts, advisories, and directives are to be disseminated, system or network administrators, personnel
Tests that may be conducted for ML1: Organization processes for employing, updating, and configuring malicious code protection mechanisms, organizational process for addressing false positives and resulting potential impact, mechanisms supporting or implement malicious code protection mechanisms (including updates and configurations), mechanisms supporting or implementing malicious code scanning and subsequent actions

Maturity Level 1 (ML1) Preparation Questionnaire

Questions:

What is the procedure to be notified of anti-malware software updates?

Is anti-malware software updated regularly on all FCI devices?

What mechanism is used to manage anti-malware?

SI.1.213 - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
CMMC Clarification - Companies should use anti-malware software to scan and identify viruses in their computer systems, and have a plan for how often scans are conducted. Real-time scans will look at the system whenever new files are downloaded, opened, and saved. Periodic scans check previously saved files against updated malware information.
Objectives for this control: Determine if the frequency for malicious code scans is define, malicious code scans are performed with the defined frequency, real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed
Things that may be examined for ML1: configuration management procedures, procedures addressing malicious code protection, malicious code protection mechanisms, records of malicious code protection updates, system configuration settings and associated documentation, scan results from malicious code protection mechanisms, record of actions initiated by malicious code protection mechanisms in response to malicious code detection ,system audit logs
People that may be interviewed for ML1: System or network administrator, personnel with information security responsibilities, personnel installing, conjuring, and maintaining the system, personnel with responsibility for malicious code protection, personnel with configuration management responsibility
Tests that may be conducted for ML1: Organizational processes for employing, updating, and configuring malicious code protection mechanisms, organization process for addressing false positives and resulting potential impact, mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations), mechanisms supporting or implement malicious code scanning and subsequent actions.

Questions:

What is the procedure to scan devices/media on FCI processing devices?

Is anti-virus installed on all FCI processing devices, and scanned regularly?

What mechanism is used to manage anti-virus

Maturity Level 1 (ML1) Preparation

Step 2: Inventory of Digital Assets

A digital asset are things of value to the operation of a business conducting DoD contracting that are owned by the business, but have no physical presence - an inventory of them is required, and a description of how and where this data is backed up is necessary. For the purposes of CMMC, an inventory of the devices these assets are stored on is also necessary.

Digital Asset Examples (not all inclusive list)

- Federal Contract Information
- Documentation From Federal Contracts
- Payment information From Federal Contracts
- Lists of Contact Information – name, location, who has access, backup
- Documented Business Processes – name, location, who has access, backup
- Intellectual Property – name, location, who has access, backup
- E-mail repositories – name, location, who has access, backup
- Virtual Property – name, location, who has access, backup
- Patents & Trade Secrets – name, location, who has access, backup
- Designs – name, location, who has access, backup
- Databases – name, location, who has access, backup
- Knowledge – name, location, who has access, backup
- Software – name, location, who has access, backup
- Credit card information – name, location, who has access, backup

List your organization's Digital Assets

IT Asset Examples (not all inclusive list)

- FCI Desktop Inventory - locations, vendors, operating systems, serial numbers
- FCI Laptop Inventory - locations, vendors, operating systems, serial numbers
- FCI Tablet Inventory - locations, vendors, operating systems, serial numbers
- FCI Network Server Inventory - locations, vendors, operating systems, serial numbers
- FCI Mobile Phone Inventory - locations, vendors, operating systems, serial numbers
- FCI Printer Inventory - locations, vendors, operating systems, serial numbers
- FCI Network Switch Inventory - locations, vendors, operating systems, serial numbers
- FCI Network Router Inventory - locations, vendors, operating systems, serial numbers
- FCI Firewall Inventory - locations, vendors, operating systems, serial numbers
- FCI Wireless Access Point Inventory - locations, vendors, operating systems, serial numbers
- FCI Wireless Controller Inventory - locations, vendors, operating systems, serial numbers
- FCI Internet Provider - Names, speeds, locations
- FCI Email Provider - Vendor, location
- FCI Cloud Service Provider - Name, Subscriptions, Services, Cost
- FCI Applications - Vendors, versions, Subscriptions, Cost (include anti-virus, malware, management software)
- FCI Data Backup - Vendors, versions, schedules, Subscriptions, Locations, Cost
- FCI Physical Access - IP Video Surveillance vendor, IP door controller vendor, IP badge reader controller
- FCI IP Phones - Vendor, location of handsets
- FCI IP Video Surveillance Cameras - locations, vendors, operating systems, serial numbers

List your organization's IT Assets

Maturity Level 1 (ML1) Preparation

Step 3: Gap Assessment

Cybersecurity is characterized by the many different types of businesses and business practices, complexity of the enterprise network and connected infrastructure, and the need to mitigate cyber risk. A PTAC or their client can attempt to conduct a GAP assessment (and there are many companies that advertise services to start at this step (usually called readiness assessment) with your CMMC certification), but not using a resource that is versed in cybersecurity consulting and auditing raises the risk of failure when assessed by a CMMC auditor. A business owner would hire an expert electrician if they needed wiring fixed, go to a good doctor if they were sick, or taken their car to the dealership for repairs, but when it comes to their computers, they try to get by with the absolute minimum. Remember, CMMC at all levels is a compliance issue (pass/fail), and the certification is required to do business with the DoD. If the decision is made to get an outside resource, explore IT/CMMC as a service. This lets a small business pay a monthly operational expense (OPEX) to outsource their IT/CMMC. As a service allows a business to concentrate on their core competency - while not having to deal with a large capital expenditure (CAPEX). If you are a sub-contractor to a prime, coordination/collaboration should be taking place during this process - as it will have a direct impact on your certification. In some situations, controls can be met by the prime and extended to the sub-contractor.

In short, a gap assessment consists of mapping the control requirement to how you are meeting it today - and what needs to be done for certification. Steps 1 - 3 cover the information required to use in a gap assessment - but knowledge of cybersecurity best practices, and security audits is required to successfully create the output from it, which is used to build the implementation plan to get your business CMMC certified.

Step 4: Implementation Plan

Implementation is the process that turns identified gaps in each security control into actions. A formal implementation plan could contain a work breakdown structure with tasks, resources, stakeholders, timeline, communication plan, etc The implementation plan plays a large role in the success of CMMC certification.

A business should have all it due diligence done prior to finalizing this plan. Costs for hardware, software, services, subscriptions, etc should be fixed.

Step 5: Assessment Package

Finally! Your business is ready to be assessed - but how does an auditor have any context to your business processes, and how ML1 controls are applied to them? This is where an assessment package comes in. An assessment package explains to the auditor things like what your business is, what type of contracts it does, information flow, audit log locations, policies, etc.

An auditor should be able to review the assessment package, examine a sample of objects for each control, interview pertinent personnel for each control, and test mechanisms for each control. The easier you make an auditor's job, the higher chance you have at achieving certification. An auditor can be scheduled at this point through the CMMC-AB Marketplace.

Maturity Level 1 (ML1) Preparation Questionnaire

Step 6: Certification

Your business has been audited, and any write ups have been satisfied within 90 days. You will be notified that it has been successfully entered into the DIB database as certified - and can now be awarded DoD contracts. Your certification is good for 3 years.

Step 7: Certification Maintenance

You thought you were finished? The auditor has merely taken a point in time picture for your certification - you are expected to maintain all controls until the next assessment in 3 years. You will be expected to have artifacts that you have been doing them and improving them in the meantime. Remember the 3 pillars of a project have been cost, performance, and schedule - and now cybersecurity? CMMC isn't a one time thing, and you don't want to do a heavy lift to be certified again in 3 years.

If you require any assistance in your CMM certification journey.

RD Risk Advisors experts stand ready to assist with all aspects of this checklist. Call or email us anytime, RD Risk Advisors is here to guide your business through the CMMC process. Please complete this questionnaire as much as possible, save and forward it to us at RD Risk Advisors. If you prefer to schedule a phone call click the logo below.

PTAC Information		DoD Contractor Information	
Name:		Name:	
Title:		Title:	
Email:		Email:	
Phone:		Phone:	