HOW-TO GUIDE

ACHIEVING CYBERSECURITY MATURITY MODEL CERTIFICATION V2.0 (CMMC) LEVEL 1

WHITE PAPER

Abstract

This How-to Guide is prepared by the Certified CMMC Assessors and Instructors at Linqs. The purpose of this white paper is to navigate and assist various size of government contractors which are preparing for the Cybersecurity Maturity Model Certification (CMMC) Level 1 certification and self-assessment.

Linqs GRC Solutions @Web @LinkedIn @Twitter

Achieving CMMC Level 1

CMMC level 1 focuses on the protection of Federal Contract Information (FCI) and is about "performing" the basic cybersecurity hygiene. Level 1 self-assessment methodology follows a data-centric security process and does not require development of a specific policy and procedure, unless a requirement calls for a particular documentary evidence. One of the documentary pieces of evidence is your asset inventory. As such, all users, processes acting on behalf of the users, people resources (i.e., contractors, vendors, ESP/MSP employees), technology resources (i.e., computers, servers, network appliances, security appliances, on-premise software, cloud-based software), and buildings/facilities must be documented.

What are the CMMC Level 1 requirements?

AC.L1-3.1.1: Authorized Access Control

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Consideration factors:

Define all of your users, processes, and devices separately, and limit their access to exactly what they are supposed to do or execute, nothing more. You should be in a position of answering "Yes" for both of these questions:

1. *Is a list of authorized users maintained that defines their identities and roles?*
2. *Are account requests authorized before system access is granted?*

Expectations to meet this requirement:

1- Having a list of all active and inactive users (i.e., employees, contractors, visitor accounts, service provider accounts, etc.), account names and where and what exact machines, applications, and services that they are authorized to access. Applications that are accessed include on-premise and cloud-based/hosted applications, including but not limited to e-mail, CRM, ERP, accounting and office/productivity applications. User accounts are disabled when the user is no longer required to access, such as when an employee leaves, pause or termination of a contractor and MSP services, etc.

2- Having a list of all devices, workstations, laptops, security protection devices, routers, wireless access points, and network appliances with unique device names, and the user accounts who are authorized to access and use these devices. Devices are removed from the network and boundary if they are no longer needed.

3- Having a complete list of all processes and system tasks and the accounts that those processes/tasks utilize. Processes must be disabled or removed if no longer needed.
4- Demonstrated process that all users, devices, and processes are regularly reviewed by the system administrators and approved before use. Users should not be able to login without a valid password which is strong and regularly changed. Users should not be allowed to access the devices/machines or run processes that they are not authorized to. Users also should not be allowed to access work applications using their personal unapproved devices, or through unauthorized network devices, such as WiFi hot spots.

AC.L1-3.1.2: Transaction & Function Control

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Consideration factors:

Define an access control list where you identify the administrators, privileged role owners, and regular users, and limit their access to applications and data based on their roles. You should be in a position of answering "Yes" for both of these questions:

1. *Are access control lists used to limit access to applications and data based on role and/or identity?*
2. *Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools)?*

Expectations to meet this requirement:

1. Having an access control list identifying all users, their roles, and the functions and tasks they are allowed to execute on workstations, machines, laptops, servers, network devices, and security protection devices. As a default, all users must be assigned only non-admin roles unless their job function specifically requires an elevated role.
2. Demonstrated process and configurations where regular users are not allowed to carry administrator rights on their workstations/laptops, and are authorized to execute only the tasks that are expected from their job.
3. File and folder permissions are configured correctly to limit the access of unauthorized users.

AC.L1-3.1.20: External Connections

Verify and control/limit connections to and use of external information systems.

Consideration factors:

Define the scope and boundary where FCI is handled and mark all IT resources and systems outside of that boundary as external. Control and limit the connections to external systems, and don't mix and share the resources. You should be in a position of answering "Yes" for the following questions:

1. *Are all connections to external systems outside of the assessment scope identified?*
2. *Are external systems (e.g., systems managed by contractors, partners, or vendors; personal devices) that are permitted to connect to or make use of organizational systems identified?*
3. *Are methods employed to ensure that only authorized connections are being made to external systems (e.g., requiring log-ins or certificates, access from a specific IP address, or access via Virtual Private Network (VPN))?*
4. *Are methods employed to confirm that only authorized external systems are connecting (e.g., if employees are receiving company email on personal cell phones, --Is your organization checking to verify that only known/expected devices are connecting)?*
5. *Is the use of external systems limited, including by policy or physical control?*

Expectations to meet this requirement:

1. A network diagram properly showing the scope and boundary of the system environment that will process and store the FCI and possible external systems connected to the system environment.
2. A policy and physical controls (e.g., web access block, closing ports, MAC and IP level controls) are in place to prevent access to external systems thereby reducing the possibility of leak of the FCI.
3. List of contractors, external service providers, and vendors as well as personal devices which are authorized to connect from external systems to the secure workspace, and existences of physical controls to control their access, such as firewalls, and VPN.

AC.L1-3.1.22: Control Public Information

Control information posted or processed on publicly accessible information systems.

Consideration factors:

Control and limit the access to public systems and sites and have a documented process to review and approve the posts/uploads. You should be in a position of answering "Yes" for the following question:

> *Does information on externally facing systems (i.e., publicly accessible web sites, social media, file sharing sites, etc.) have a documented approval chain for public release?*

Expectations to meet this requirement:

1. A documented process listing the individuals who are authorized to post/upload on public systems, as well as individuals to review and approve the post/upload. How the review process is conducted to remove potential FCI should be explained in the process.
2. A demonstrated example of review to ensure that the process is followed.
3. A demonstrated example of timely removal of FCI in case it is found in the posted/uploaded document/data.

IA.L1-3.5.1: Identification

Identify information system users, processes acting on behalf of users, or devices.

Consideration factors:

You should be in a position of answering "Yes" for the following questions:

1. *Are unique identifiers issued to individual users (e.g., usernames)?*
2. *Are the processes and service accounts that an authorized user initiates identified (e.g., scripts, automatic updates, configuration updates, vulnerability scans)?*
3. *Are unique device identifiers used for devices that access the system identified?*

Expectations to meet this requirement:

> Documentation or configuration files to support that each user, process, and device have its own unique identifier (i.e., username, MAC Id, process Id, etc.) and credentials, such as passwords when accessing the system.

IA.L1-3.5.2: Authentication

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Consideration factors:

You should be in a position of answering "Yes" for the following questions:

1. *Are unique authenticators used to verify user identities (e.g., passwords)?*
2. *Can your show that the organization maintains a record of all service accounts (such as scripts, etc.) when reviewing log data or responding to an incident?*
3. *Are user credentials authenticated in system processes (e.g., credentials binding, certificates, tokens)?*
4. *Are device identifiers used in authentication processes (e.g., MAC address, non-anonymous computer name, certificates)?*

Expectations to meet this requirement:

1. Documentation or configuration files to support that each user, process, and device have its own unique identifier (i.e., username, MAC Id, process Id, etc.) and credentials, such as passwords when accessing the system.
2. All users, devices, processes (including the company mobile devices) are forced to have strong passwords. Default passwords are not used and immediately changed.
3. Demonstrated configuration and log files that authentication process applies to all users, devices, services accounts, and processes.
4. Devices and processes have enabled automatic logout or lock features due to inactivity.

MP.L1-3.8.3: Media Disposal

Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Consideration factors:

You should be in a position of answering "Yes" for the following question:

> *Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable?*

Expectations to meet this requirement:

Any media, such as computer hard-drive, mobile device, flash drive, CDs/DVDs, as well as documents containing FCI must be erased, encrypted, shredded, or destroyed before they are disposed or recycled. Demonstrated process to show one of the accepted sanitization methods is used in the organization:

a. Crushing and destroying the media module
b. Encrypting the data inside with a long (16+ character) key
c. Overwriting the data many times using a special program
d. Degaussing the media module
e. Shredding the documents and CD/DVD with cross-cut shredders

PE.L1-3.10.1: Limit Physical Access

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Consideration factors:

This requirement is about the physical access to facility, machines, equipment, and system components which can store, process or generate FCI.

Expectations to meet this requirement:

1. List of personnel, including contractors and vendor employees who access your facility, is developed and facility access credentials are issued.
2. The areas where FCI is handled are identified and marked accordingly.
3. Physical security protection methods are in place, such as guards, locks, cameras, and card readers to limit the access to sensitive areas. Only those who are identified and authorized can access with their own badges/key cards/keys.
4. FCI processing/handling machines (computers, laptops, operating machines, servers, network appliances) and printers are all located inside the protected areas. If printer is outside of the secured area, its use must be initiated by an authorized person after login (i.e., on-demand encrypted printing). No FCI should be sent to a printer for an instant printing if the printer is outside of the protected area.
5. Doors to protected/secure areas are self-closing and locking.
6. No network wiring passes through the unsecured areas.

PE.L1-3.10.3: Escort Visitors

Escort visitors and monitor visitor activity.

Consideration factors:

You should be in a position of answering "Yes" for the following questions:

1. *Are personnel required to accompany visitors to areas in a facility with physical access to organizational systems?*
2. *Are visitors clearly distinguishable from regular personnel?*
3. *Is visitor activity monitored (e.g., use of cameras or guards, reviews of secure areas upon visitor departure, review of visitor audit logs)?*

Expectations to meet this requirement:

1. Demonstrated process of visitors being escorted.
2. Visitors are given a different color or type of badge to distinguish them, and their use of the badge is enforced.
3. A visitor log exists with a necessary information captured, such as their names, contact information, company worked, visited person name, time in/out.
4. Visitor activity is further monitored with cameras and/or guards.

PE.L1-3.10.4: Physical Access Logs

Maintain audit logs of physical access.

Consideration factors:

You should be in a position of answering "Yes" for the following questions:

1. *Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements?*
2. *Are visitor access records retained for as long as required?*

Expectations to meet this requirement:

1. A visitor log exists with minimally necessary information captured, such as names, company worked, visited person name, time in/out. Visitor logs are retained per company record retention policy, which should typically be not less than a year.
2. In addition to visitor access, all access to the secure areas must be logged by the access control devices and logs are retained in a secure place for the retention period.

PE.L1-3.10.5: Manage Physical Access

Control and manage physical access devices.

Consideration factors:

You should be in a position of answering "Yes" for the following questions:

1. *Is the inventory of physical access devices maintained (e.g., keys, facility badges, key cards)?*
2. *Is access to physical access devices limited (e.g., granted to, and accessible only by, authorized individuals)?*
3. *Are physical access devices managed (e.g., revoking key card access when necessary, changing locks as needed, maintaining access control devices and systems)?*

Expectations to meet this requirement:

1. An inventory of physical access devices, such as keys, badges, and key cards.
2. A secure location for keys, badges, and keycards where access is authorized only to identified persons.
3. A process outlining how the access devices are maintained and updated, period of updates, etc. Electronic keycards are considered one of the best as regular keys will need to be changed when an employee/contractor leaves.

SC.L1-3.13.1: Boundary Protection

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.

Consideration factors:

Your system environment must be isolated from external systems using firewalls, gateways, and cloud service boundaries if you are using cloud service. You should consider addressing the following questions:

1. *What are the external system boundary components that make up the entry and exit points for data flow (e.g., firewalls, gateways, cloud service boundaries)?*
2. *What are the internal system boundary components that make up the entry and exit points for key internal data flow (e.g., internal firewalls, routers, any devices that can bridge the connection between one segment of the system and another) that separate segments of the internal network?*
3. *Is data flowing in and out of the external and key internal system boundaries monitored (e.g., connections are logged and able to be reviewed, suspicious traffic generates alerts)?*
4. *Is data traversing the external and internal system boundaries controlled such that connections are denied by default and only authorized connections are allowed?*
5. *Is data flowing in and out of the external and key internal system boundaries protected (e.g., applying encryption when required or prudent, tunneling traffic as needed)?*

Expectations to meet this requirement:

1- System network diagram clearly showing the internal and external system boundaries, details of segmentation, internal system components (i.e., servers, computers, workstations, network and security appliances, mobile devices, printers, etc.), and location of networking appliances and security protection assets (i.e., firewalls, IDS, DLP, end-point protection software, anti-virus software, etc.)
2- Demonstrated existence of working security protection and monitoring devices at the boundaries.
3- Configuration and log files of the firewalls and other protection devices:
   a. Configuration files show that all connections are denied by default and only authorized connections are allowed by firewall rules. Ports and applications are blocked as a default unless needed.
   b. Demonstrated process where configuration, log files, and alerts are regularly reviewed.

SC.L1-3.13.5: Public-Access System Separation

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Consideration factors:

If any of your internal system components needs to be reached by the public they must be identified and separated from the other parts of the internal network by sub networking. Accepted physically/logically separation methods include isolated subnetworks and dedicated VLAN segmentation such as Demilitarized Zone (DMZ).

Expectations to meet this requirement:

All publicly accessible system components are listed. These would include web server, e-mail server, file server, VPN gateways, and other publicly accessible servers/devices. System network diagram shows the sub networking and/or dedicated VLAN (i.e., DMZ) to separate those components. Firewalls are installed and configured in correct locations.

SI.L1-3.14.1: Flaw Remediation

Identify, report, and correct information and information system flaws in a timely manner.

System hardware, software, and firmware bugs and issues should be identified and fixed timely. There must be a pre-defined frequency (in terms of days) for conducting vulnerability scans, configuration reviews, and a timeline for correcting the issues.

Consideration factors:

1- *Is the time frame (e.g., a number of days) within which system bug and issue identification activities (e.g., vulnerability scans, configuration scans, manual review) must be performed defined and documented?*
2- *Are system bugs and issues (e.g., vulnerabilities, misconfigurations) identified in accordance with the specified time frame?*
3- *Is the time frame (e.g., a set number of days dependent on the assessed severity of a flaw) within which system bugs and issues must be corrected defined and documented?*
4- *Are system flaws (e.g., applied security patches, made configuration changes, or implemented workarounds or mitigations) corrected in accordance with the specified time frame?*

Expectations to meet this requirement:

1- A document and configuration files defining the time frame for review of bug and issues, software patches, configuration scans, and vulnerability scans.
2- Log files showing the reported issues and bugs were fixed, configuration changes were done, and software patches were installed in predefined timeline.
3- Obsolete and old hardware and software with no vendor support are disabled and no longer used.

SI.L1-3.14.2: Malicious Code Protection

Provide protection from malicious code at appropriate locations within organizational information systems.

Meeting this requirement is as easy as installing a robust anti-virus software on all end-points, including computers, workstations, servers, mobile devices, and all other machines as defined in-scope.

Consideration factors:

Are system components (e.g., workstations, servers, email gateways, mobile devices) for which malicious code protection must be provided identified and documented?

Expectations to meet this requirement:

1- A document listing all in-scope system components where malicious code (e.g. virus, trojan, worm, ransomware, etc.) protection software is installed.
2- *Best practice:* Use an office/productivity software where malicious software removal function is embedded for automatic scanning of the documents, spreadsheets, downloaded files, e-mails, etc.
3- If a cloud service is used, obtain information/certification from the service provider that hosted files are subject to regular malicious code scanning.

SI.L1-3.14.4: Update Malicious Code Protection

Update malicious code protection mechanisms when new releases are available.

This requirement would be satisfied by configuring all installed anti-virus software to be regularly updated and observing the update process performed successfully.

Consideration factors:

Is there a defined frequency by which malicious code protection mechanisms must be updated (e.g., frequency of automatic updates or manual processes)?

Expectations to meet this requirement:

1- A document or configuration file defining the frequency by which anti-virus software are updated, either via automatic updates or manually.
2- Demonstrated process of regular updates on the malicious code scanning software exists, and updates are accessible and subscribed by the organization. Anti-virus software typically receives the latest virus signatures as well as other AI based virus detection algorithms from the vendor servers directly, as such devices should be enabled to connect to vendor servers.

SI.L1-3.14.5: System & File Scanning

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Consideration factors:

Are files from media (e.g., USB drives, CD-ROM) included in the definition of external sources and are they being scanned?

Expectations to meet this requirement:

1- A document or configuration files showing the frequency of scans.
2- Demonstrated process of malicious code scanning on all devices on pre-defined periods.
3- Demonstrated process of real-time malicious code scanning on files when they are received from external resources (i.e., internet, external media, USB drives, etc.), when they are opened or executed.

About Linqs™

Linqs is a leading provider of Governance, Risk, and Compliance (GRC) training, software and advisory services to corporations and organizations. Our experts, trainers, and consultants have the knowledge and vast experience to solve the complex compliance issues faced by the high-tech industries. What makes us also different are our customer focus and our dedication to customer satisfaction.

Select Linqs for your most challenging training, process development and assessment/audit need in the following areas:

Information Security & Cybersecurity

- Policy & Procedure Development
- Cybersecurity Maturity Model Certification (CMMC) Preparation
- ISO 27001 Compliance
- PCI DSS Compliance
- SOC 2/3 Reporting
- NIST Cybersecurity Framework
- NIST 800-171 Compliance
- NIST 800-53 Compliance
- Audit

Data Privacy

- Policy & Procedure Development
- ISO 27701 Compliance
- GDPR Compliance
- CCPA Compliance
- Audit

Know Your Customer/Vendor & 3rd Party Risk Software

- Denied & Restricted Party Screening Software
- On-demand vendor & customer screening service

Export & ITAR Compliance

- Export Compliance Program Development
- Product & Technology Export Classification
- ITAR Technology Control Plan
- DFARS Compliance
- Sanctions review
- License Application
- Audit