Joel Recane, RPO, CCP
Sr. Cybersecurity Engineer

CMMC Level 1: Process, Pitfalls, and Practical Steps to Success

September 23, 2025

About Stratus

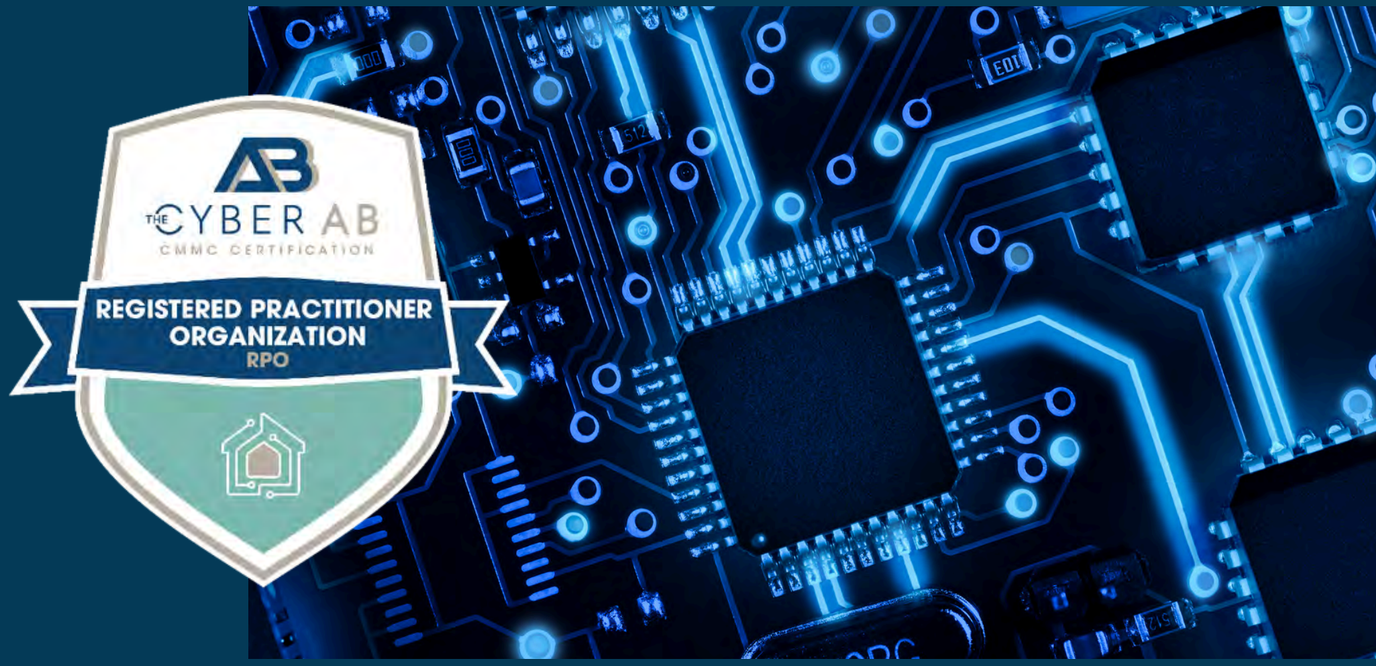
Joel Recane, RPO, CCP
Sr. Cybersecurity Engineer

CMMC-AB RPO since 2022

Multiple RPs, RPAs & CCP on staff

Guided one of the first 85 orgs through a successful CMMC L2 audit

Performing our internal CMMC L2 audit this fall



STRATUS SERVICES

CMMC Updates

The '48 CFR rule' which requires DoD contracting officials to require CMMC compliance before awarding DoD contracts will be made **effective on Nov 10th, 2025**, making CMMC Level 1 mandatory on that date.

Sept 2025

Level 1 Overview

Does Level 1 apply to you?

Sept 2025

The basic components of CMMC Level 1

Scoping: Understand proper scope

Focuses on the protection of Federal Contract Information. (32 CFR § 170.4 and 48 CFR § 4.1901)

Assessment Process: choose your route

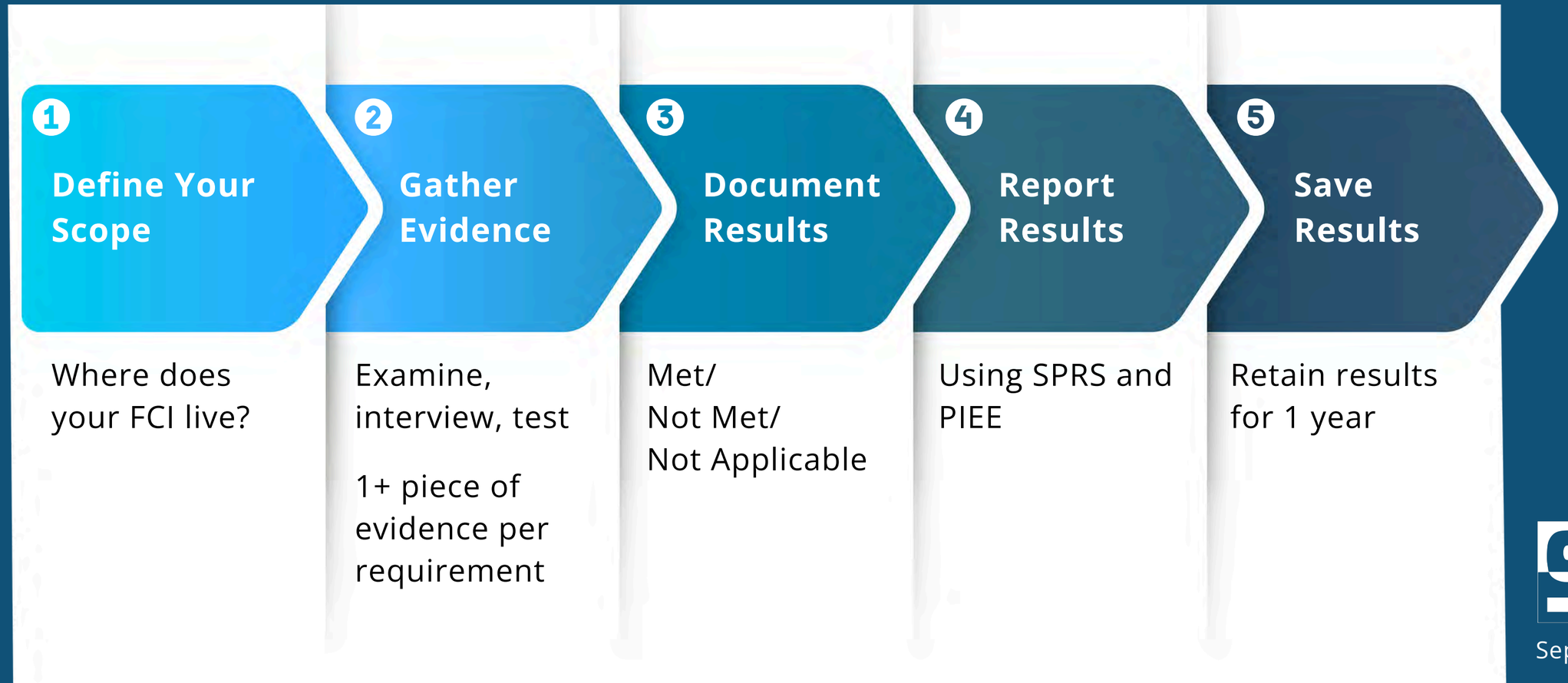
Can be completed as an internal assessment or can be completed by a third party contractor

---

Review controls: Requirements vs Assessment Objectives

Includes 15 basic safeguarding requirements, as specified in FAR 52.204-21

Level 1 Self-Assessment Steps



Sept 2025

Scoping

Scoping is the most important step to proper CMMC Compliance.

Assets

- In Scope – Process/Store/Transmit FCI
- Specialized Assets – GFE/IoT/OT/Test Equipment
- What is Out-of-Scope?

Additional Factors

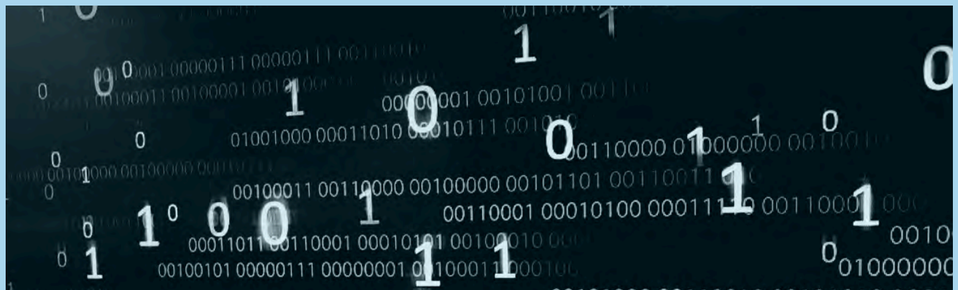
- People
- Technology
- Facilities
- External Service Providers

Sept 2025

Federal Contract Information (FCI)

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

32 CFR § 170.4 and 48 CFR § 4.1901



Sept 2025

Assessment Process

Components of a proper Level 1 Assessment

- System Security Plan (SSP)
  - Is this required?
- Third Party Assessment or Self-Assessment?
- Requirements vs Assessment Objectives

Sept 2025

Assessment Process

Components of a proper Level 1 Assessment

- Evidence
  - “To verify and validate that an OSA is meeting CMMC requirements, evidence needs to exist demonstrating that the OSA has fulfilled the objectives of the Level 1 requirements….” - CMMC Assessment Guide Level 1
- Assessment Criteria and Methodology
  - Interview
  - Examine
  - Test
- Assessment Findings
  - Met
  - Not Met
  - Not Applicable

Sept 2025

Reporting Assessment Results

Sept 2025

Supplier Performance Risk System

"[S]upports DoD Acquisition Professionals with meeting acquisition regulatory and policy requirements"

Procurement Integrated Enterprise Environment

"[T]he primary enterprise procure-to-pay (P2P) application for the Department of Defense and its supporting agencies"

Resources:

- https://www.sprs.csd.disa.mil/pdf/CMMCQuickEntryGuide.pdf
- https://www.sprs.csd.disa.mil/pdf/CMMCL2SelfQuickEntryGuide.pdf
- https://pieetraining.eb.mil/wbt//xhtml/wbt/portal/overview/vendorRegister.xhtml
- https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml

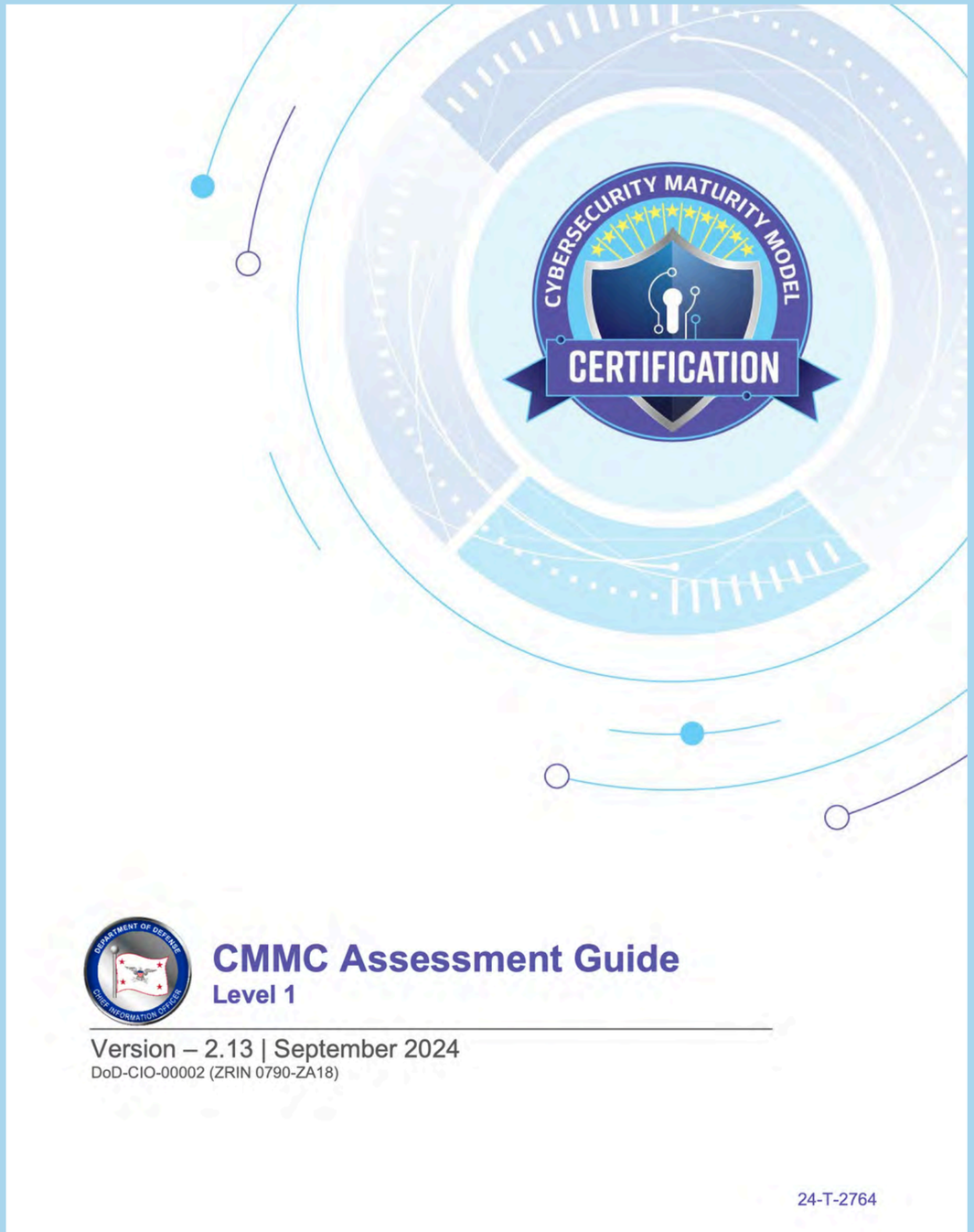
Controls

- AC – Access Control
- IA – Identification and Authentication
- MP – Media Protection
- PE – Physical Protection
- SC – System and Communications Protection
- SI – System and Information Integrity

Sept 2025

Completing the Assessment

Assessment Guide:
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf



Sept 2025

Requirements vs Assessment Objectives

EXAMPLE: SI.L1-B.1.XII – FLAW REMEDIATION [FCI DATA]

Requirement

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements

Assessment Objectives

A set of determination statements that, taken together, expresses the desired outcome for the assessment of a security requirement.

Sept 2025

Requirements vs Assessment Objective

AC.L1-B.1.I – AUTHORIZED ACCESS CONTROL [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. authorized users are identified;
b. processes acting on behalf of authorized users are identified;
c. devices (and other systems) authorized to connect to the system are identified;
d. system access is limited to authorized users;
e. system access is limited to processes acting on behalf of authorized users; and
f. system access is limited to authorized devices (including other systems).

Requirements vs Assessment Objective

AC.L1-B.1.II – TRANSACTION & FUNCTION CONTROL [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. the types of transactions and functions that authorized users are permitted to execute are defined; and

b. system access is limited to the defined types of transactions and functions for authorized users.

Requirements vs Assessment Objective

AC.L1-B.1.III – EXTERNAL CONNECTIONS [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. connections to external systems are identified;
b. the use of external systems is identified;
c. connections to external systems are verified;
d. the use of external systems is verified;
e. connections to external systems are controlled/limited; and
f. the use of external systems is controlled/limited.

Requirements vs Assessment Objective

AC.L1-B.1.IV – CONTROL PUBLIC INFORMATION [FCI DATA]

Assessment Requirement

Control information posted or processed on publicly accessible information systems.

Assessment Objectives

Determine if:

a. [a] individuals authorized to post or process information on publicly accessible systems are identified;
b. [b] procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified;
c. [c] a review process is in place prior to posting of any content to publicly accessible systems;
d. [d] content on publicly accessible systems is reviewed to ensure that it does not include [FCI]; and
e. [e] mechanisms are in place to remove and address improper posting of [FCI].

Requirements vs Assessment Objective

IA.L1-B.1.V – IDENTIFICATION [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. system users are identified;
b. processes acting on behalf of users are identified; and
c. devices accessing the system are identified.

Requirements vs Assessment Objective

IA.L1-B.1.VI – AUTHENTICATION [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. the identity of each user is authenticated or verified as a prerequisite to system access;
b. the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and
c. the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

Requirements vs Assessment Objective

MP.L1-B.1.VII – MEDIA DISPOSAL [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. system media containing [FCI] is sanitized or destroyed before disposal; and
b. system media containing [FCI] is sanitized before it is released for reuse.

Requirements vs Assessment Objective

PE.L1-B.1.VIII – LIMIT PHYSICAL ACCESS [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. authorized individuals allowed physical access are identified;
b. physical access to organizational systems is limited to authorized individuals;
c. physical access to equipment is limited to authorized individuals; and
d. physical access to operating environments is limited to authorized individuals.

Requirements vs Assessment Objective

PE.L1-B.1.IX – MANAGE VISITORS & PHYSICAL ACCESS [FCI DATA]

Assessment Requirement

Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

Assessment Objectives

Determine if:

a. visitors are escorted;
b. visitor activity is monitored;
c. audit logs of physical access are maintained;
d. physical access devices are identified;
e. physical access devices are controlled; and
f. physical access devices are managed.

Requirements vs Assessment Objective

SC.L1-B.1.X – BOUNDARY PROTECTION [FCI DATA]

Assessment Requirement

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.

Assessment Objectives

Determine if:

a. the external system boundary is defined;
b. key internal system boundaries are defined;
c. communications are monitored at the external system boundary;
d. communications are monitored at key internal boundaries;
e. communications are controlled at the external system boundary;
f. communications are controlled at key internal boundaries;
g. communications are protected at the external system boundary; and
h. communications are protected at key internal boundaries.

Requirements vs Assessment Objective

SC.L1-B.1.XI – PUBLIC-ACCESS SYSTEM SEPARATION [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. publicly accessible system components are identified; and
b. subnetworks for publicly accessible system components are physically or logically separated from internal networks.

Requirements vs Assessment Objective

SI.L1-B.1.XII – FLAW REMEDIATION [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. the time within which to identify system flaws is specified;
b. system flaws are identified within the specified time frame;
c. the time within which to report system flaws is specified;
d. system flaws are reported within the specified time frame;
e. the time within which to correct system flaws is specified; and
f. system flaws are corrected within the specified time frame.

Requirements vs Assessment Objective

SI.L1-B.1.XIII – MALICIOUS CODE PROTECTION [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. designated locations for malicious code protection are identified; and
b. protection from malicious code at designated locations is provided.

Requirements vs Assessment Objective

SI.L1-B.1.XIV – UPDATE MALICIOUS CODE PROTECTION [FCI DATA]

Assessment Requirement

Update malicious code protection mechanisms when new releases are available.

Assessment Objectives

Determine if:

a. malicious code protection mechanisms are updated when new releases are available.

Requirements vs Assessment Objective

SI.L1-B.1.XV – SYSTEM & FILE SCANNING [FCI DATA]

Assessment Requirement

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

Assessment Objectives

Determine if:

a. the frequency for malicious code scans is defined;
b. malicious code scans are performed with the defined frequency; and
c. real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Pitfalls

- Improper scoping
- Misinterpreting requirements
- Lack of evidence

CMMC “Leveling Up”

Transitioning from Level 1 to 2 is a difficult process

- Level 1 only has 15 of the 110 controls form Level 2
- Different rules for scoping
- FedRAMP required for Cloud Service Providers
- Much more Technical

Sept 2025

Questions?

Contact us:

Email **cmmc@stratus-services.com**
Phone **(907) 272-4730**
Web **www.stratus-services.com**

Sept 2025